Network Camera

IP2111/2121

User's Manual

User's Manual User's Manua

Product name:	Network Camera (IP21x1)
Release Date:	2005/07/06
Manual Revision:	2.00
Web site:	www.vivotek.com
Email:	technical@vivotek.com sales@vivotek.com
Made in Taiwan.	©Copyright 2000-2005. All rights reserved

Before You Use

It is important to carefully examine the contents with the Chapter Package Contents after opening the package. If there is anything missing, contact your reseller. Read the Chapter Physical Description before assembling and operating the device and peripherals. Understanding the physical description can prevent damage caused by abnormal usage and reduce most problems during installation.

Basically Network Camera is a network device and should be easy to use for those who already have basic network knowledge. If there is a system error and it does not recover easily due to erroneous configuration, read the System recovery section in Appendix Troubleshooting to restore factory default settings and perform installation again.

Network Camera has been designed for various environments and can be used to build various applications for general security or demonstration purposes. For standard applications, find the appropriate section in the Chapter How to Use for your application and follow the steps to setup the system. To make best use of Network Camera, read Chapter Advanced Functions to get creative ideas and review Chapter System Configuration for detailed explanations of system configurations. To those professional developers, the Appendix URL Commands of Network Camera will be a very helpful reference to develop a Web-based application.

Surveillance devices may be prohibited by law in your country. Though Network Camera is not only a high performance surveillance system but also a networked video server, ensure that the operations of such devices are legal before installing this unit for surveillance.

Those paragraphs preceding with must be fully understood and cautioned. Ignoring the warnings may result in serious hazards.

Table of Contents

Before You Use 2

Package Contents 5

Features and Benefits 6

Physical Description 8

Rear Panel 8

How to Install 12

Ethernet Environment 13
Software configuration 15
Modem Environment 20

How to Use 29

Authentication 29
Installing Plug-in 30
Main Page 31

System Configuration 34

Introduction 34
Setup Wizard 35

Application Wizard 35

Definitions of Configuration 36

Advanced Functions 48

Capture Up-to-date Still Images 48
Uploading Snapshots Periodically 51
Customize Graphics in Homepage 52
Command Script for Complex Applications 53
URL for External Device Control 56
URL of System Maintenance 58
Configure System via FTP 59
Telnet Commands 65

Appendix 67

A. Troubleshooting 67
B. Frequently Asked Questions.....68
C. Upgrade System Firmware 72
D. URL Commands of Network Camera 73
E. Camera Control Cable 84
F. Time Zone Table 85
G. Technical Specifications 88

Package Contents

If any of the following items are missing, please contact your reseller.

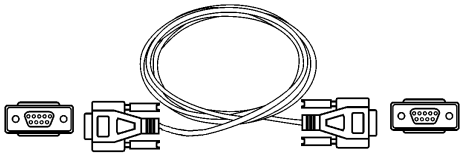
☑ Network Camera IP2111/IP2121

☑ Power adapter

☑ I/O terminal connector

☑ CS Ring and wrench

☑ Null modem cable

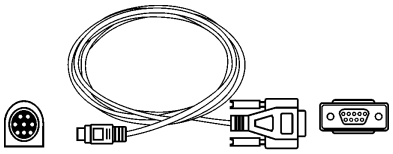


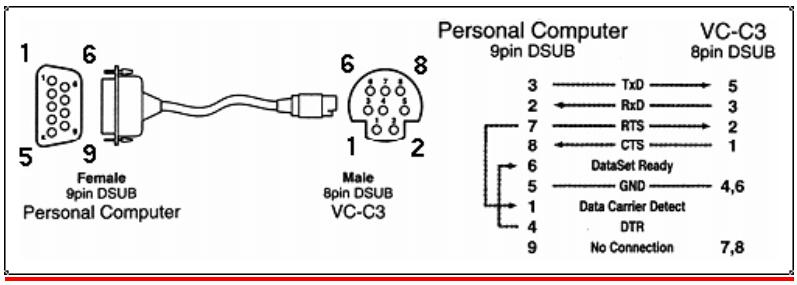
☑ Software CD

☑ Quick installation guide

☑ Warranty

☑ Camera control cable





Features and Benefits

Network Camera is a high-performance networking video transmitter. With powerful VLIW DSP core and fully optimized algorithm, it can compress and transmit the high quality real-time video through standard TCP/IP inter-network. In addition to meet the basic needs of video feed, many advanced features are added to help building applications of surveillance or web attraction. The state-of-art design well compromises among stable, robust, simple-to-use and flexibility.

☆ Real-time motion-JPEG compression

Video input can be efficiently compressed into packets of JPEG images without delay. Optimal compression engine makes the equivalently excellent image with much smaller size. There is no more sacrifice in remote monitoring and storage. Five levels of compression ratio and three sizes of image resolutions are easy to meet your requirement.

☆ Robust system operation

Industrial real-time operating system prevents from malicious hackers and virus that threat Windows or Linux systems. The on-board watchdog eternally monitors the system operations for dead-proof.

☆ Easy Web access via standard browser

You don't have to install any software to access Network Camera. The embedded Web server makes users can access Network Camera anywhere over Internet with any popular Web browser. As long as you are connected to network, you can cast your eyes on your precious property.

☆ Password protection of system access

Password level protection is provided by the system to prevent from malicious intruders from network. Once the password of administrator is entered, any user will need password authentication to access Network Camera. Each user can have individual access right to view video or control external devices.

☆ Built-in motion detection

No more external sensors are required. The video channel can be setup to detect any motion with customized settings. By tuning the object size and sensitivity, it is more

reliable to fit into your environment. With this built-in facility, you can easily setup a security system in your home or office.

☆ Weekly schedule for automatic surveillance

The user-defined time period will repeat weekly to check any security settings and accordingly sending notification or drive external devices. It is easy to install in SOHO, retail shop and home as a security system.

☆ Flexible I/O control for external devices

There is one opto-isolated sensor input and one relay output to control external devices. System integrators can easily replace the current analog systems to build an advanced security system.

☆ Bundled powerful surveillance software

To extend the capabilities of Network Camera, a powerful surveillance program is included in the package and totally free to use. Users can easily utilize the existing PC to be a digital video recorder. Schedule or one-click recording keep every important moment in your local hard disk; reliable motion detection and instant warning make you sharp for every conditions. Quick and simple search and playback let you easily find the moment you want to inspect more carefully and output to AVI files for another copy.

☆ Remote system upgrade

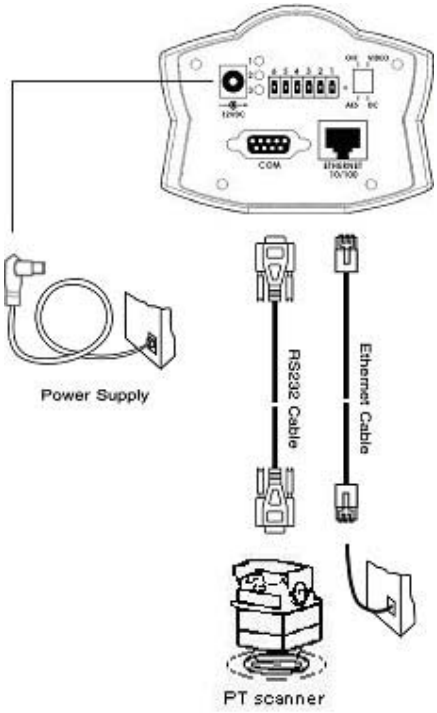
To achieve the promise we made to support our valuable customers in life-time, the most up-to-date firmware is always put on our web site to add new functions or solve known bugs. A free upgrade wizard is included to facilitate the job.

☆ Developer’s technical support

The high-performance Network Camera can be integrated into many applications under perfect control of budget. The complete programming interface and standard JPEG format can ease and speed developers’ task. More creative ideas can be found on our Web site.

Physical Description

Rear Panel



Status LED's

Each time Network Camera starts up, it will perform power-on-self-test, abbreviated as POST, to examine every hardware module. As soon as the administrator plugs in the power connector both LED's under the power LED will flash one by one until the diagnosis is done. If the result is good, both status LED's will turn off for a while and then follows the pattern below. If any module fails, refer to the Appendix A for the error pattern and follow the trouble-shooting procedures. If the system still cannot operate normally, please contact your reseller for technical service.

Network Interface	Condition	LED2 (Heartbeat)	LED3 (Status)
Ethernet	before installed	OFF	OFF
	after installed	flash	OFF
	during camera control	flash	Flash
PPP with modem	after POST	flash	ON
	before connected	ON	ON
PPP with null modem	after connected	flash	ON

	before installed	OFF	OFF
	after installed	flash	OFF

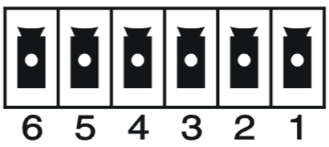
Ethernet 10/100 socket

Connect to an Ethernet network with a UTP category 5 cable of length shorter than 100 meters according to the standard. Once the Ethernet cable is connected without error, Network Camera will utilize the Ethernet interface prior to the modem attached to COM2.

COM port

This RS232 serial port can connect with a modem or included null modem cable to utilize dial-up network when Ethernet is not available. If Network Camera operates with Ethernet interface, administrators may use this port to control PT scanner attached to VIDEO.

General I/O terminal block



1	←	DI+	INPUT	(Max. 50mA, 12VDC)
2	←	DI-	INPUT	
3	←	SW_COMMON	OUTPUT	(short with NC at initial state)
4	←	SW_NOPEN	OUTPUT	(Max. 1A, 24VDC or 0.5A, 125VAC)
5	←	RS485 B		(inverting)
6	←	RS485 A		(non-inverting)

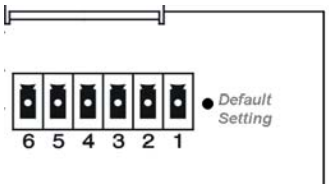
Network Camera provides a very flexible general I/O interface to combine with the user's security devices such as sensors, alarms, lighting or door locks. The general I/O terminal block has six pins for device control. These pins can be divided into two categories based on their functions, including RS485 and digital input and output.

If the device connected to COM has an RS485 interface, wire two control lines to pin 5 and pin 6. After switching to RS485 on the configuration page, the PT scanner control commands will be directed through pin 5 and pin 6. If the distance from the controlled

device is too far to allow accurate function, an external power source may be used to pull high the RS485 signal.

Network Camera provides one digital input and one relay switch. Pin 1 and pin 2 can be connected to external sensor and the state of voltage will be monitored according to the programmed scripts in configuration. The relay switch can be used to turn on or off external devices.

Restore button



There is a button hidden in the box for restoring the system factory default settings. When the system fails to install or operates abnormally, use the included assistant stick in the package and follow the following procedures to reset the system back to its original status.

Poke the assistant stick into the hole to press down on the restore button. Restart the system by unplugging and re-plugging the power jack. While keeping the button pressed, the system will perform POST twice rather than the usual once, which can be observed from the flashing LEDs. After the system flashes the LEDs for the second time, withdraw the stick to release the button. The system will have restored factory default settings at that moment.

Auto Iris Lens Connector

If the auto iris lens is used, AES on rear panel must be turned OFF. And you also have to select VIDEO Drive or DC Drive lens by the switch.
The pin assignment of the auto iris lens connector is as follows:

	VIDEO Drive	DC Drive
Pin 1	Power source	Damp-
Pin 2	Video signal	Damp+
Pin 3	Not used	Driver+
Pin 4	Ground, Shield	Driver-

Power adapter

Connect the power jack of the included power adapter. Connecting the power adapter should be the last operation while physically installing Network Camera.

The power adapter of Network Camera and the external power supply are prohibited to exist together. Only one source can feed power to Network Camera. Improper usage will result in serious damage.

How to Install

To easily fit into various environments, Network Camera automatically detects the attached interfaces and configures itself to the best condition. Therefore users need not care how to select the network between Ethernet and modem, and whether the Ethernet speed is 10Mbps or 100 Mbps. The high performance built-in CCD and lens always give users delicate image quality.

Network Camera supports Ethernet and modem interfaces according to the user's existing network. Ethernet can provide higher bandwidth to achieve the best performance while dial-up network with modem is more common in current Internet applications. Refer to the related installation section for your network environment. If both interfaces are available, Ethernet is recommended and will be chosen as the first priority if Ethernet cable and modem are concurrently attached. Managing to install in the other interface will automatically clear the previous network settings to start new installation.

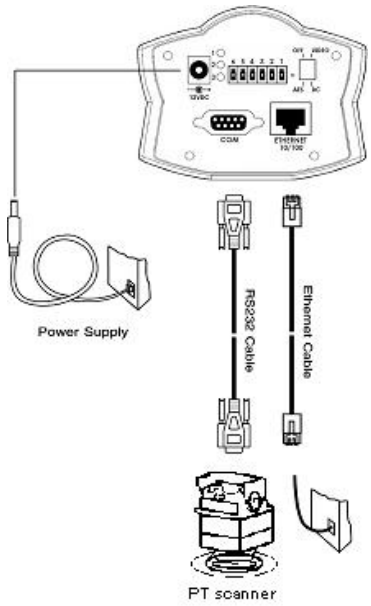
In the following content, "**user**" refers to those who can access Network Camera and "**administrator**" means the supervisor who has the root password to configure Network Camera in addition to general access. Administrators should carefully read this manual, especially during installation.

Ethernet Environment

Hardware installation

Before installing multiple Network Cameras at the well-chosen locations, the administrator should memorize the serial numbers on the packages respectively for future use.

Cable connection



Shut down all the peripheral devices prior to connection. Connect the supplied cables from Network Camera to related devices according to the above diagram. Note that the power adaptor must be kept unplugged until other cables are firmly connected.

Power on

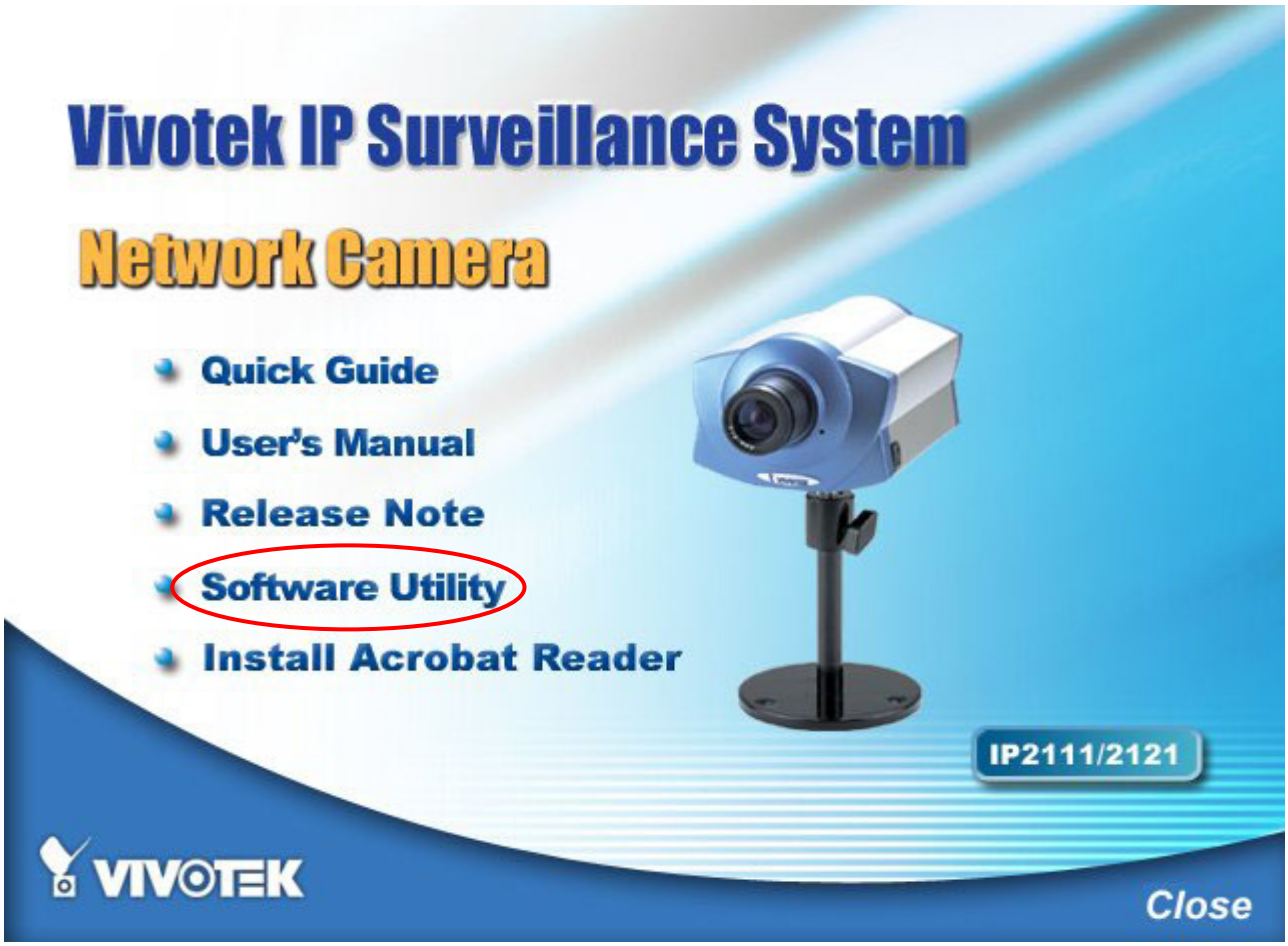
Make sure all cables are correctly and firmly connected before turning on Network Camera. Turn on cameras, sensors, alarm devices, and then attach the power adaptor of Network Camera to the electric power socket*. After the POST (power-on self test) is complete and the result is successful, Network Camera is ready for software configuration as described in this manual. At this stage, network speed and video modulation type are automatically detected. If the detection of video modulation fails, administrators may change the setting on the configuration page. Refer to the configuration section for further information.

Connect the power jack of the power adapter to Network Camera prior to plugging the utility end into the utility power socket. It will reduce accidental electric surge shock.

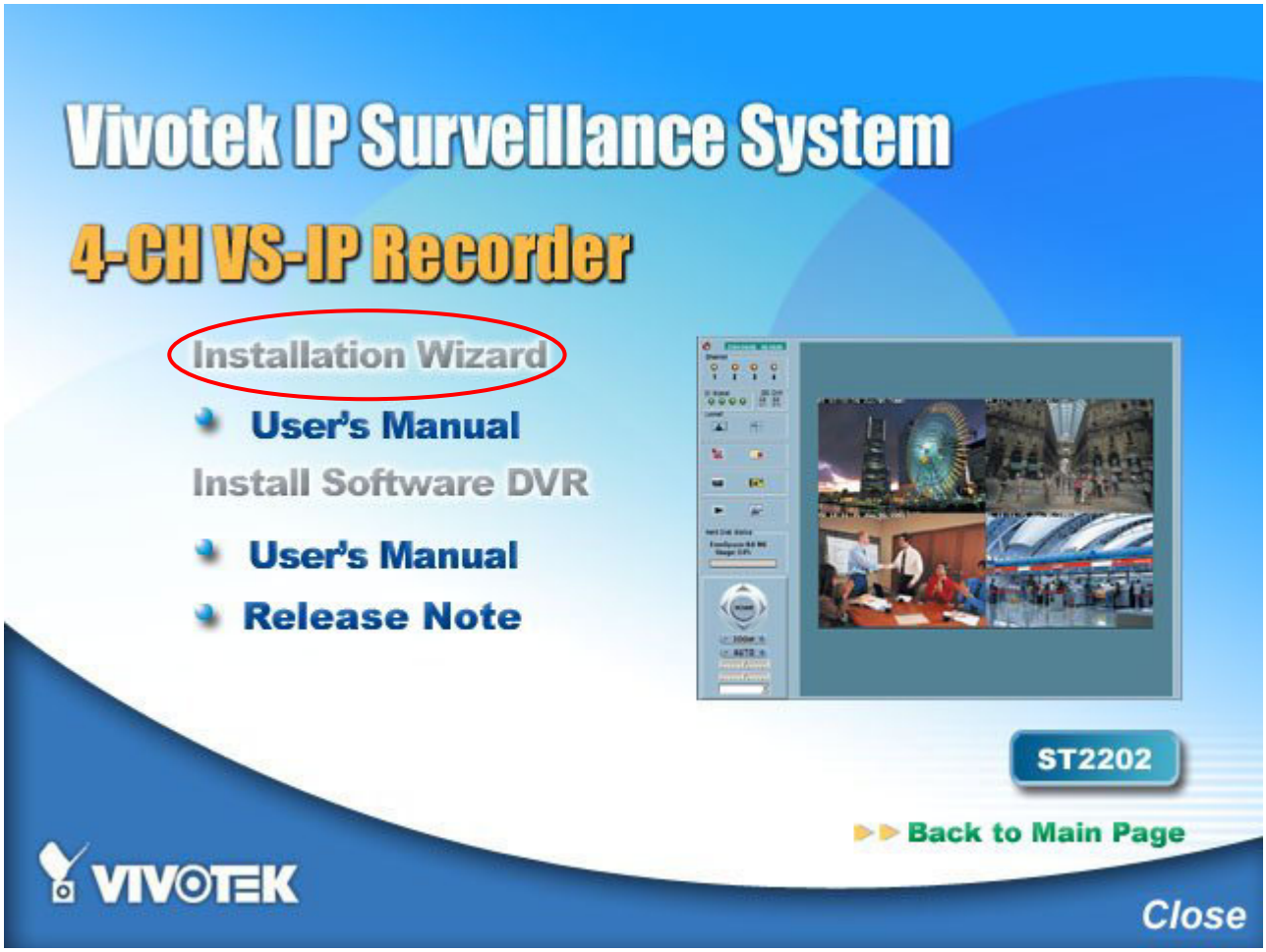
Software configuration

In this manual, "User" refers to whoever has access to the Network Camera, and "Administrator" refers to the person who can configure the Network Camera and grant user access to the camera.

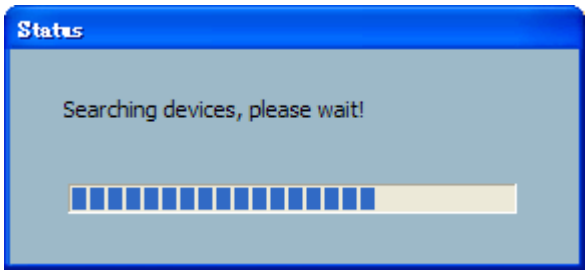
At the end of the hardware installation, the Administrator must place the product software CD into the CD-ROM drive of the PC running in MS Windows. An auto-run program will pop up (If the program is not on auto-run, go to the root directory of the software CD and click on “autorun.exe”).



Click on “Software Utility” item, after the window contains changed, click on “Installation Wizard” to run installation program.

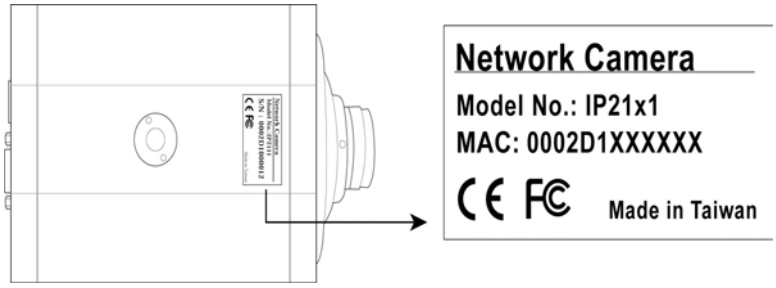


Upon Installation Wizard's start up, a searching box will pop up. This program searches for product on the same LAN:



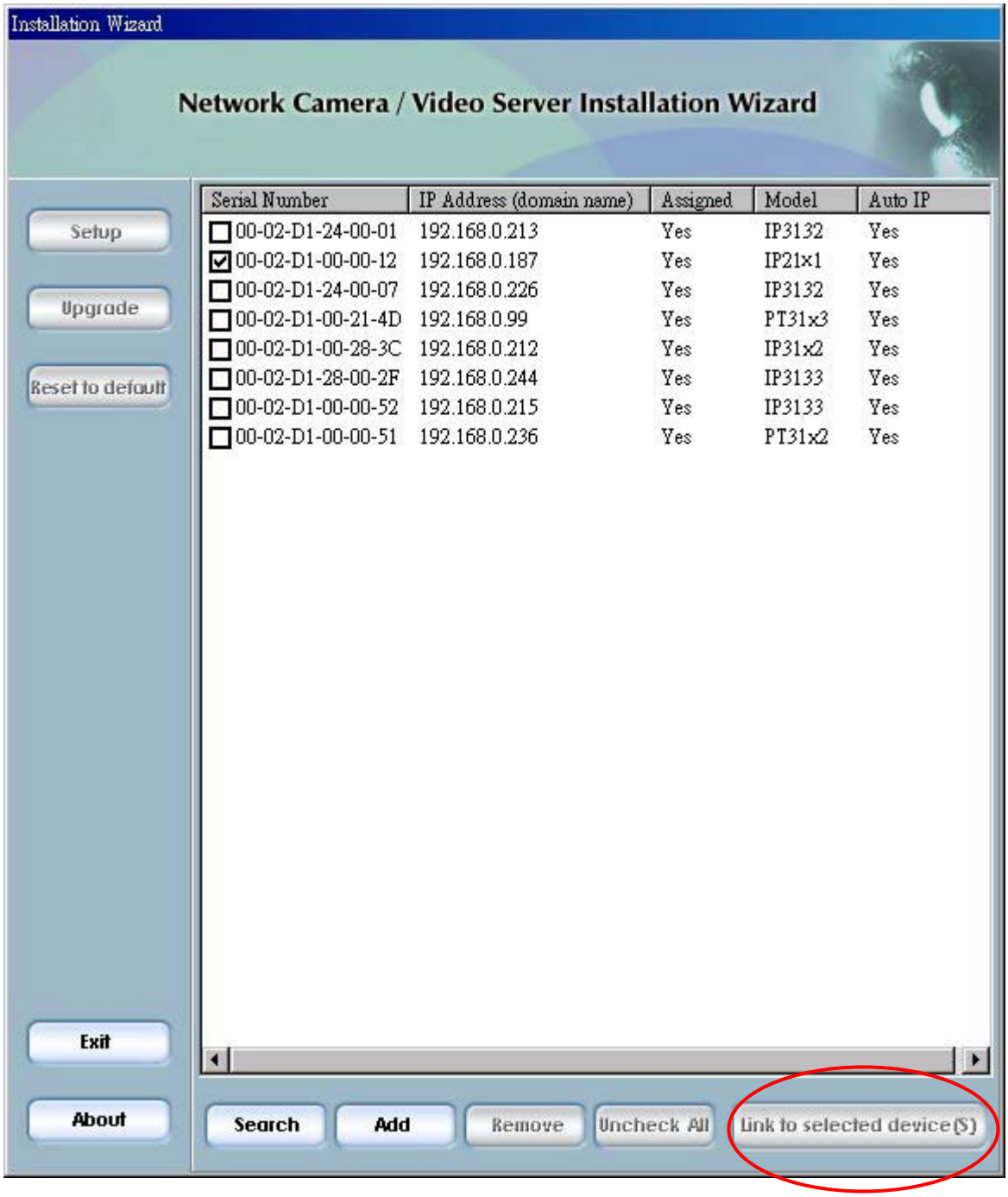
After searching, Video Servers or Network Cameras will be located by the Installation Wizard. There may be several entries shown in the window. The Administrator may differentiate the Network Cameras with the serial number.

For the series number in the "Serial Number" field, please check the label on the bottom of the camera.



The IP addresses shown in the "Current IP Address" field reflect those on the local network. They may be from the DHCP server. If there is no DHCP server, the camera will try to find a free IP address (this takes from 15 second to 3 minutes, depending on the LAN status). The method of finding IP address is seeking from 192.168.0.99, to 192.168.0.254. If any of the address inside this range is free, the Network Camera will be assigned to this IP address, and its subnet mask would be 255.255.255.0. If none of the addresses is free, the Network Camera will try the range from 192.168.0.2 to 192.168.0.98. After an IP address is assigned to the camera, the “Activity” status LED blinks.

The new UPnP function will always assign an IP address for the Network Camera. The Administrator can click on button– “Link to selected device” to connect the I.E. to the camera.
If the camera is not on the IP installer list, click on the “Search” button to search for the camera on the LAN.



For more detailed usage of the Installation Wizard, please refer to the user's manual of the Installation Wizard.

For more detailed usage of the Installation Wizard, please refer to the user's manual of the First access to Network Camera

Change initial password of administrator

Starting the Web browser to connect to the assigned IP address of Network Camera, users will be asked for user name and password by an authentication message window. A root password, identical to the Network Camera's serial number, is needed for the initial access to a newly installed Network Camera. The administrator must change the root password immediately after the initial installation to ensure security. The new root password should be well memorized since there is no way to retrieve or recover it. After changing the password, the browser will display an authentication window again to ask for the new password.

Manage user privilege

For complete protection from illegal usage, Network Camera provides three privileges and always needs user name and password before access. The lowest level is DEMO mode whose services are subject to administrator's permission. The standard level is the USER mode that consists of twenty user profiles. Each user is able to access Network Camera under the given privilege, except for system configuration. The twenty user profiles are also maintained by the administrator. The highest level is ROOT mode that only opens to administrators for initial setup, system configuration, user administration and software upgrade. The user name of the administrator is internally assigned to "**root**".

Complete the network settings

Although Network Camera already can be accessed after software installation in local area network, administrators should complete the network settings in the configuration page. The complete network configurations including subnet mask as well as the IP address of default gateway and DNS are provided by your network administrator or Internet service provider. Once the wrong network settings make Network Camera fail to work, refer to Appendix A to restore factory default settings.

By default Network Camera will need administrator's installation every time it reboots. If the network settings are sure to work all the time, disable the install option in network configuration Web page or Installer program.
Details about configurations are described in the relative category of the Chapter Definitions of Configuration.

Modem Environment

Hardware installation

Before installing Network Camera, the administrator should memorize the serial numbers on the packages respectively for the initial passwords.

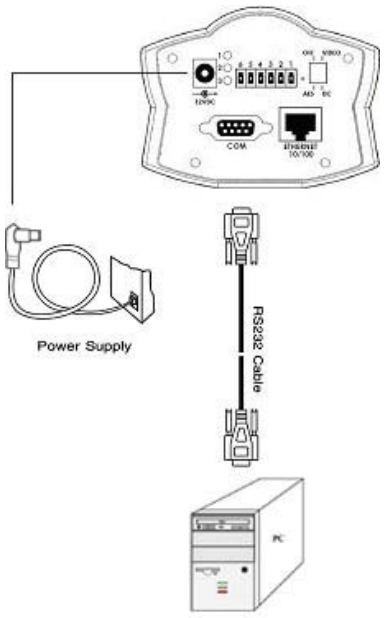
To use a dial-up network, the Ethernet socket should be left disconnected since Ethernet is the first priority among available interfaces. After powering up, Network Camera will detect if any external modem is connected to the modem port. Once a modem is detected, the heartbeat LED will flash periodically. If no modem responds, Network Camera will assume the included null modem cable is connected to perform system configuration. Then both LEDs under the power LED will turn on until null modem connection is established.

If users have setup a remote dialup server or subscribed to an ISP service, Network Camera can be configured to dial to the server upon special events. Otherwise it will wait permanently for the user's call to establish a network connection to provide services.

In the following content, dial-in connection denotes a passive Network Camera waiting for a phone call to establish a point-to-point connection. Dial-out connection denotes an active Network Camera to dial out to the other end of a dial-up server or any Internet service provider, abbreviated as ISP, to request a point-to-point connection.

Cable connection

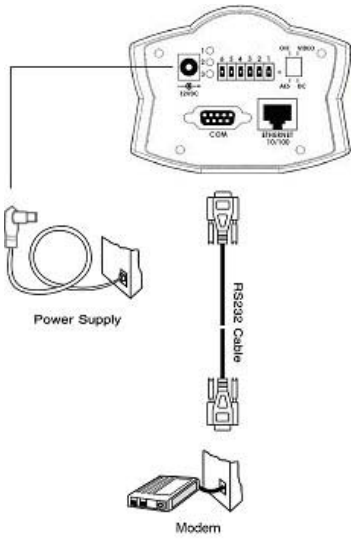
Null modem mode



Shut down the peripheral devices prior to connection and keep the power adaptor

unplugged until other cables are firmly connected. In the environment without Ethernet, administrators can use the included null modem cable to connect to Network Camera directly and access point-to-point. After necessary information is entered and saved, turn off Network Camera and remove the null modem cable. Follow the installation of modem mode in next paragraph to connect to Internet. Note Network Camera will not really reset system where it is used to in null modem mode.

Modem mode



If users have setup a remote dialup server or subscribed to an ISP service, Network Camera can be configured to dial to the server upon user-defined events. Otherwise it will wait permanently for the user's call to establish a network connection to provide services. Before installation, make sure the necessary dialing information is correctly setup via Ethernet or null modem connection.

Power on

Make sure all cables are correctly and firmly connected. Turn on cameras, sensors, alarm devices, and then finally attach power adaptor of Network Camera to the electric power outlet*. Since most automatic detections of hardware perform when the system starts, Network Camera should be turned on after all peripherals are turned on and ready.

Connect the power jack of the power adapter to Network Camera prior to plugging the utility end into a utility power outlet. It will reduce accidental electric surge shock.

Software installation

Via Ethernet

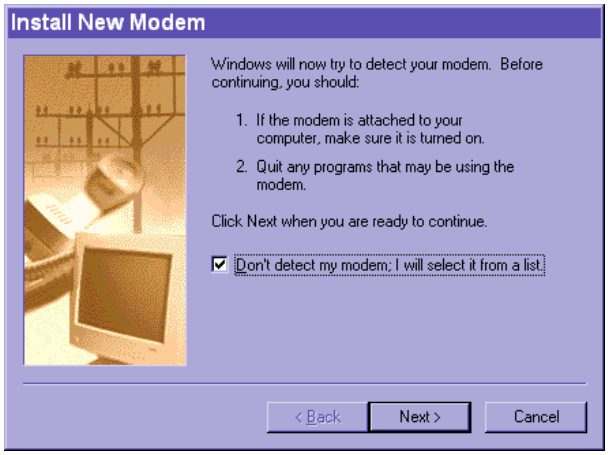
Enter the COM configuration Web page and select the driver type as modem. Well configure each field for dialing information. Refer to the COM section in Definition of Configuration for detailed description.

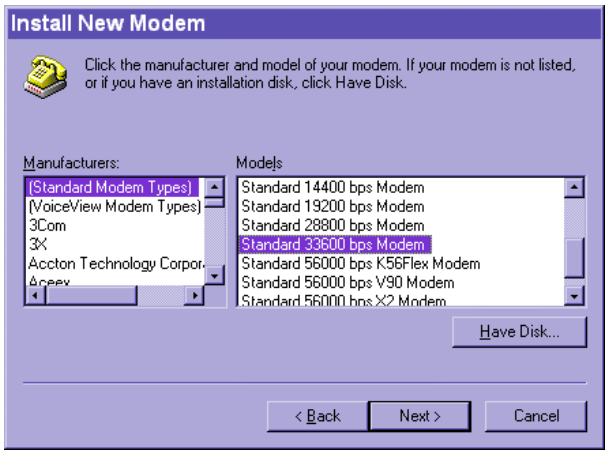
Via null modem

Install a new modem

1. Open the control panel and double click the modems icon.

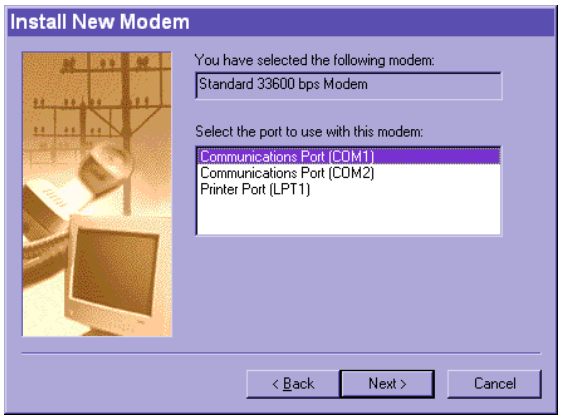
2. Check "**Don't detect my modem.....**" item and click on Next > to install a new modem.


Install New Modem
Windows will now try to detect your modem. Before continuing, you should:
1. If the modem is attached to your computer, make sure it is turned on.
2. Quit any programs that may be using the modem.
Click Next when you are ready to continue.
Don't detect my modem; I will select it from a list.
< Back
Next >
Cancel



3. From (Standard Modem Type) choose the **Standard 33600 bps Modem** and click on Next >.

4. Choose the serial port that the included null modem cable is attached to and click on Next >. The null modem is now ready for use.



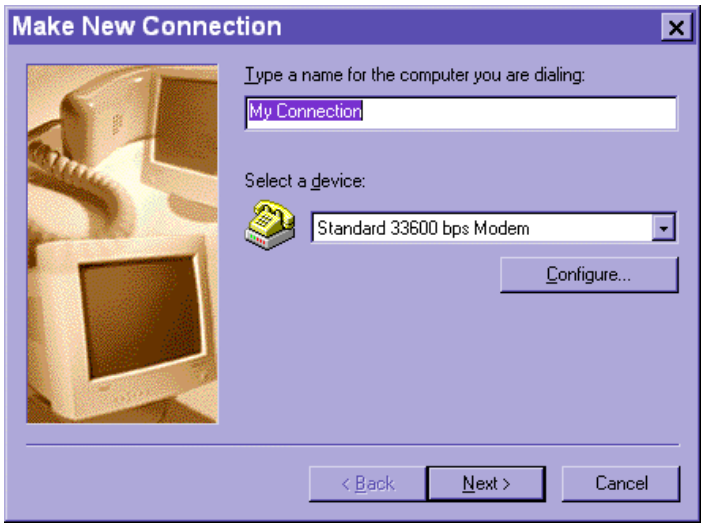
Install New Modem
Your modem has been set up successfully.
If you want to change these settings, double-click the Modems icon in Control Panel, select this modem, and click Properties.
< Back
Finish
Cancel

If no Dial-Up adapter exists in the system, Windows may automatically prompt to install. Press OK to continue. If it does not start automatically, double click the network icon in control panel to install Microsoft dial-up adapter.

Dial-Up Networking
File Edit View Go Favorites Connections Help
Back Forward Up Create Dial Cut Copy Paste Undo
Address Dial-Up Networking
Links
Make New
My Connection
Make New Connection
You have successfully created a new Dial-Up Networking connection called:
My Connection
Click Finish to save it in your Dial-Up Networking folder. Double-click it to connect.
To edit this connection later, click it, click the File menu and then click Properties.
Dial-Up Networking
Dial-Up Networking needs to install the Microsoft Dial-Up Adapter. Click OK to start installation.
OK

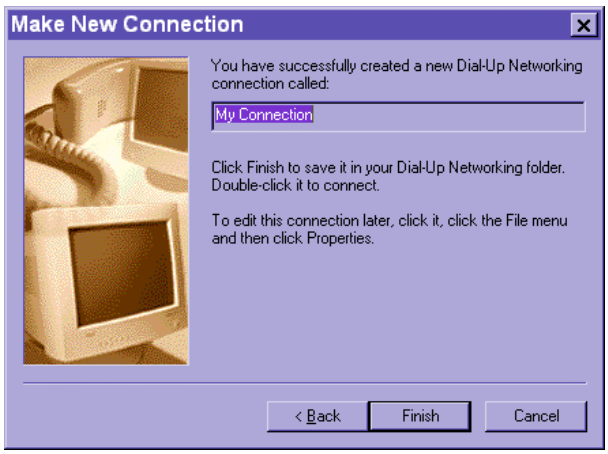
Setup a new connection

1. After the 33600 bps modem is installed, open the dialup network folder in Windows to build a new connection.



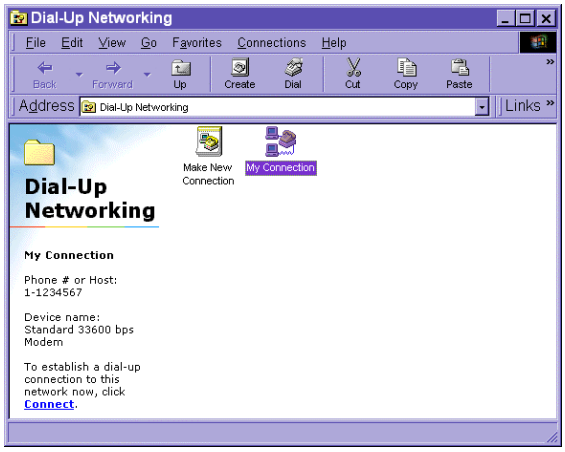
2. Select the device as the newly installed standard 33600 bps modem and click on Next >.

3. Just enter arbitrary digits as phone number and click on Next >. The phone number here is not important.

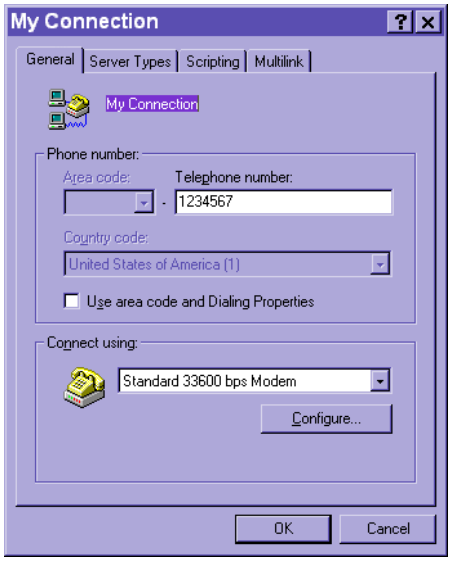

Make New Connection
You have successfully created a new Dial-Up Networking connection called:
My Connection
Click Finish to save it in your Dial-Up Networking folder. Double-click it to connect.
To edit this connection later, click it, click the File menu and then click Properties.
< Back
Finish
Cancel

4. After clicking on Finish, this new connection will display in the Dial-up Networking folder and will be used for null modem connections.

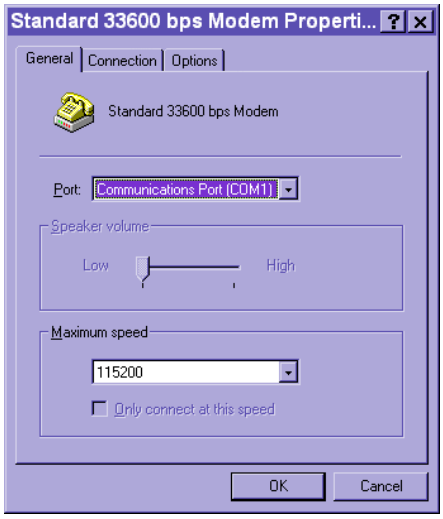
5. Right-click on the newly setup connection icon for entering properties.



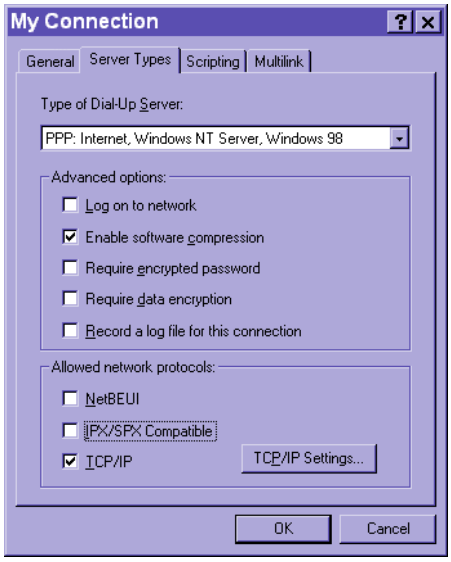
6. In the first General page, clear "**Use area code and Dialing Properties**" option and click on Configure...



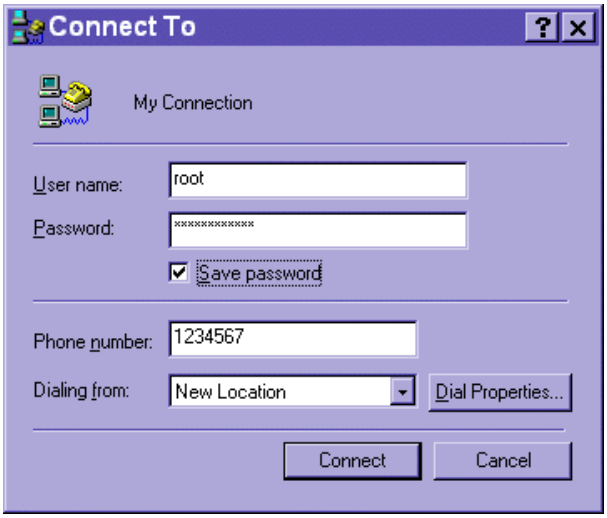
7. Select 115200 as the speed and click on OK.



8. On the second page, only check "**Enable software compression**" and "**TCP/IP**" while leaving others blank. Keep other settings as default values and click on OK.



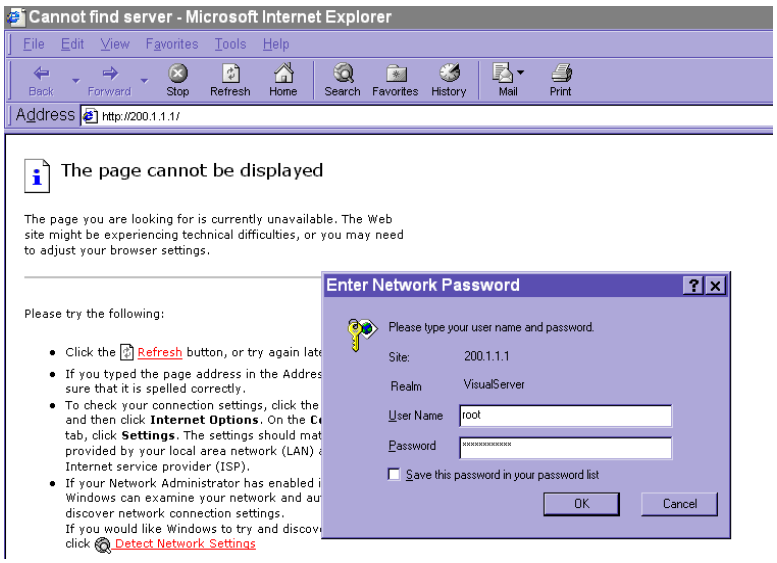
Now the connection is ready to use for null modem. Double click the newly setup connection. A dialing information window will pop up. Enter "**root**" as user name and the serial number labeled on the bottom side of the box as the password and click on Connect. Notice that the letters in the serial number should be capital form. For example, type 'A' instead of 'a'. After some negotiation prompts, a connection status window will show the speed is 115200 bps.



After connection is established successfully, go to the next section, First access to Network Camera.

If an error message indicates a hardware error while connecting for the first time, especially in Microsoft Windows 2000 environment, try again to recovery the possible detection failure.

First access to Network Camera in null modem mode


Cannot find server - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print
Address http://200.1.1.1/
The page cannot be displayed
The page you are looking for is currently unavailable. The Web site might be experiencing technical difficulties, or you may need to adjust your browser settings.
Please try the following:
Click the Refresh button, or try again
If you typed the page address in the Addres
sure that it is spelled correctly.
To check your connection settings, click the
and then click Internet Options. On the
tab, click Settings. The settings should mat
provided by your local area network (LAN)
Internet service provider (ISP).
If your Network Administrator has enabled
Windows can examine your network and au
discover network connection settings.
If you would like Windows to try and discov
click Detect Network Settings
Enter Network Password
Please type your user name and password.
Site: 200.1.1.1
Realm VisualServer
User Name root
Password
Save this password in your password list
OK
Cancel

Through direct connection by null modem cable, administrators can connect to "*http://200.1.1.1*" in the web browser. "**200.1.1.1**" will be the default IP address of Network Camera in dial-in connection; "**200.1.1.100**" will be the given IP address for the user's PC by Network Camera. The user name and password are the same as what was entered during software installation.

After successful authentication, administrators should see the motion pictures in the main page. When using Microsoft Internet Explorer, administrators must allow installing a plug-in provided by Network Camera additionally prior to viewing motion pictures.

Change initial password of administrator

For best security, administrators must change the password on the security page of configuration immediately. After changing the password, the browser will display the authentication window again to confirm the new password.

Manage user privilege

Administrators can add up to twenty user profiles in the Security option. While Network Camera accepts dial-in connection and acts as a server, the user name and password used in dialing are the same as what is stored in the user database managed for web access. Any managed user can be authorized during PPP negotiation and access web pages. However, only administrators can access the configuration page.

Complete network settings

Basically the null modem is used to setup the later attached modem where Ethernet is not available. Refer to the modem setting in the COM section for details about ISP information. After everything is set and saved, turn off Network Camera and replace the null modem cable with modem for dial-up network. Since the null modem connection is used to configure Network Camera in advance for modem connection, administrators cannot connect again without restarting the system.

First access to Network Camera in modem mode

If the dial-out is not prohibited and the attached modem is recognized, Network Camera will send out the system startup log and connection log by email or FTP according to user's settings as soon as the system is ready. That can be used to verify if the settings work. Then Network Camera will always wait for someone to dial in. To dial in Network Camera, setup a connection in dialup network on PC where the phone number is the phone line of Network Camera. After connecting successfully, start the Web browser and connect to "*http://200.1.1.1*". In this case, Network Camera runs as a dial-up server and assigns the IP address of "**200.1.1.100**" to the PC at the other end. While seeing the authentication message window, type "**root**" as user name and the serial number of Network Camera as the initial password. The point-to-point connection allows users connecting Network Camera for surveillance at any time.

If the administrator has setup some conditions in the application Web page or the script file, Network Camera will automatically dial out based on the administrator's configuration. Refer to the Application section in the Chapter Definitions of Configuration for special security applications.

How to Use

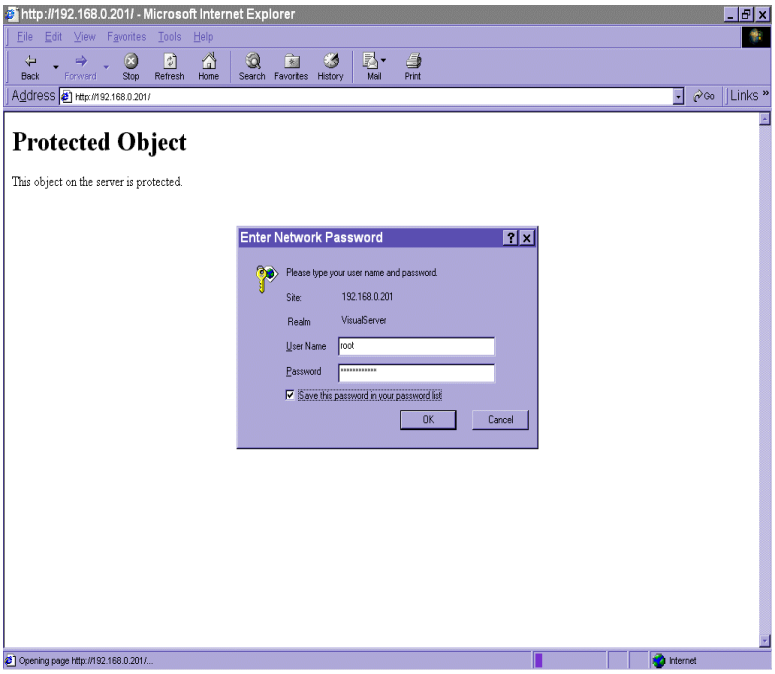
Open your familiar web browser and connect to Network Camera just like a general web site and the video will present on demand. Make sure the web address of the target Network Camera is accurate.

Authentication

After opening the Web browser and typing in the URL of Network Camera, a dialogue window will pop out to request a username and password. For administrator's initial usage of Network Camera, enter the username as "**root**" and the password as the serial number in capital letters. The serial number can be found on the labels under the body of Network Camera and the top side of the carton. The primary users will be allowed to enter as soon as the administrator finishes adding user profiles. Upon successful authentication, the main page will be displayed.

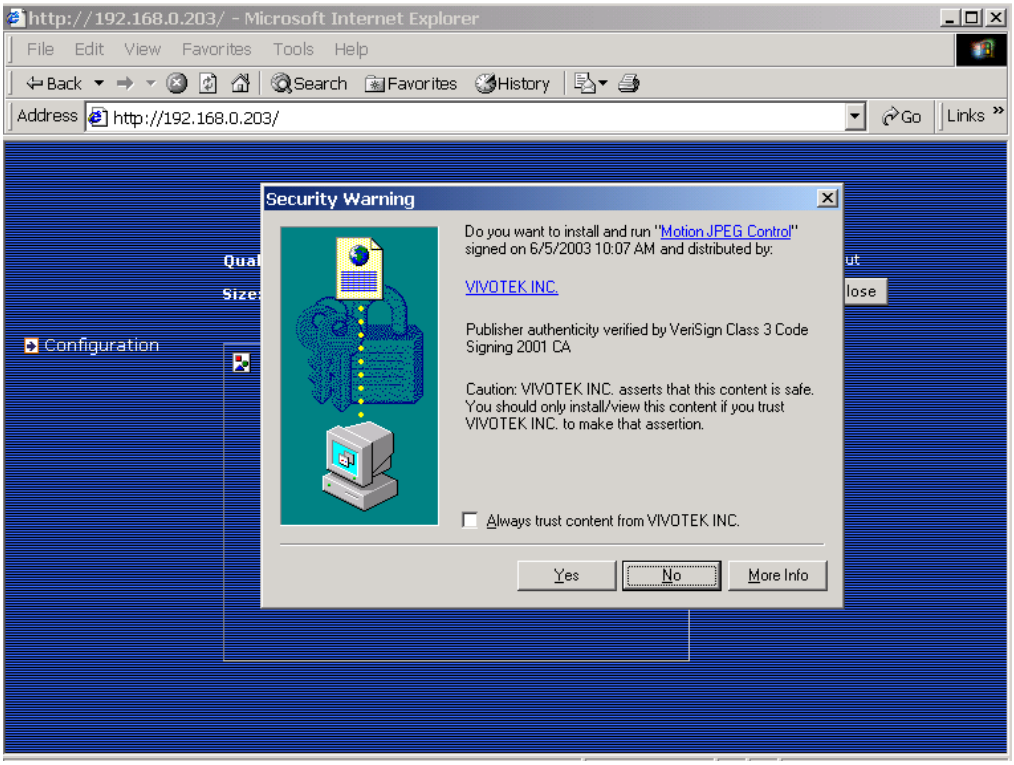
For demonstration purpose, enter the Security Web page of configuration to activate the demo account and choose permitted services. Once the demo account is setup, any one may watch the video by using "**demo**" as user name while ignoring the password. Different from primary users, the demo account has certain limitations that are determined by administrators.

In the figure, the foreground is the login window and the background shows the message when authentication fails. The user may check the option to save the password for future convenience.



Installing Plug-in

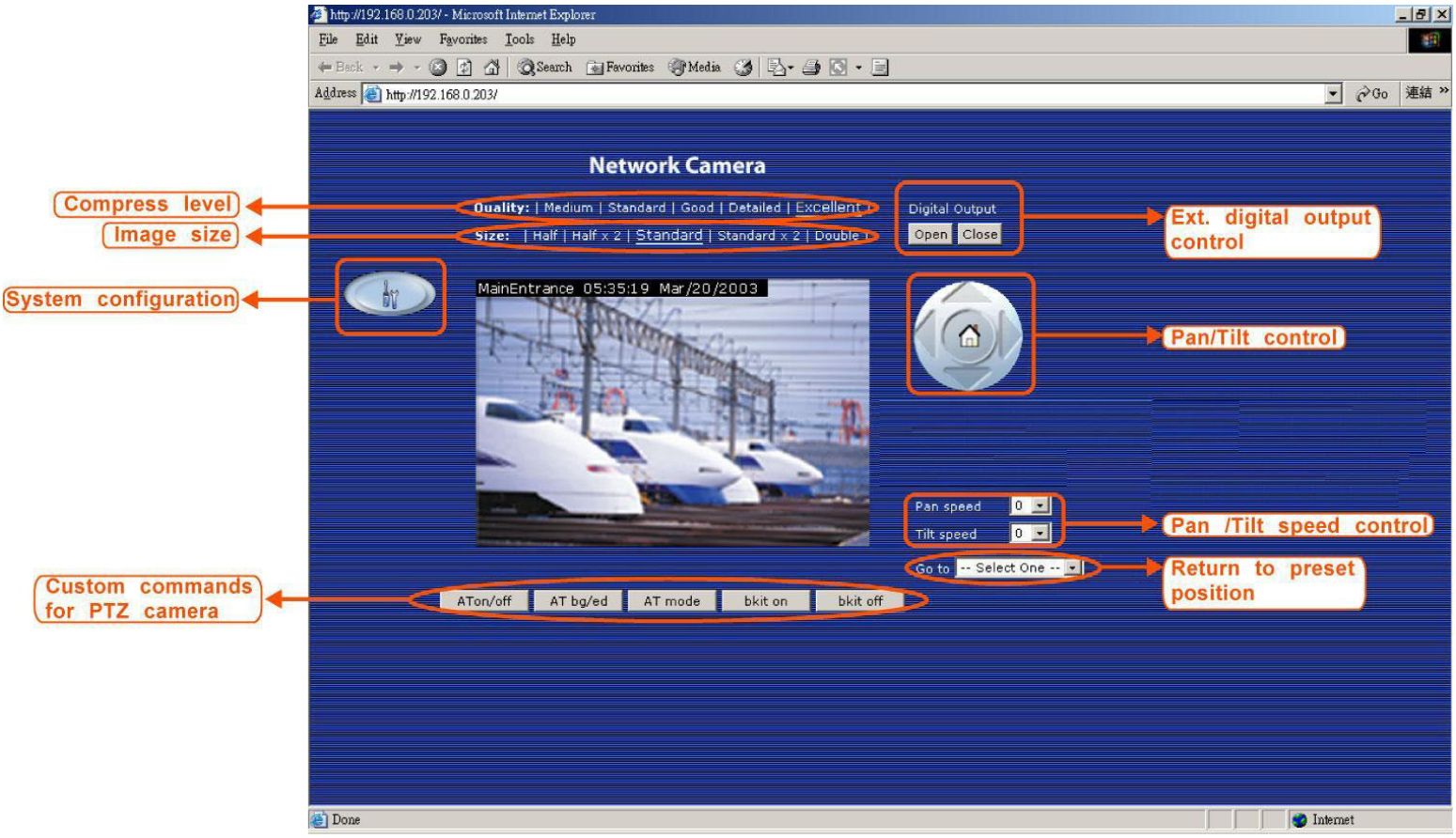
If it is initial access to Network Camera via the Web browser supporting server push, the motioned pictures will display directly. If the Web browser is Internet Explorer in Windows, users will be asked to install a new plug-in that is provided by Network Camera. This plug-in has been registered for certificate and is used to display motioned pictures in the Internet Explorer. Users may click on Yes to install the plug-in. If the web browser does not allow the user to install, check the security option to lower security levels or contact network supervisors.


http://192.168.0.203/ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://192.168.0.203/
Go Links
Security Warning
Do you want to install and run "Motion JPEG Control" signed on 6/5/2003 10:07 AM and distributed by:
VIVOTEK INC.
Publisher authenticity verified by VeriSign Class 3 Code Signing 2001 CA
Caution: VIVOTEK INC. asserts that this content is safe. You should only install/view this content if you trust VIVOTEK INC. to make that assertion.
Always trust content from VIVOTEK INC.
Yes
No
More Info
Configuration
lose

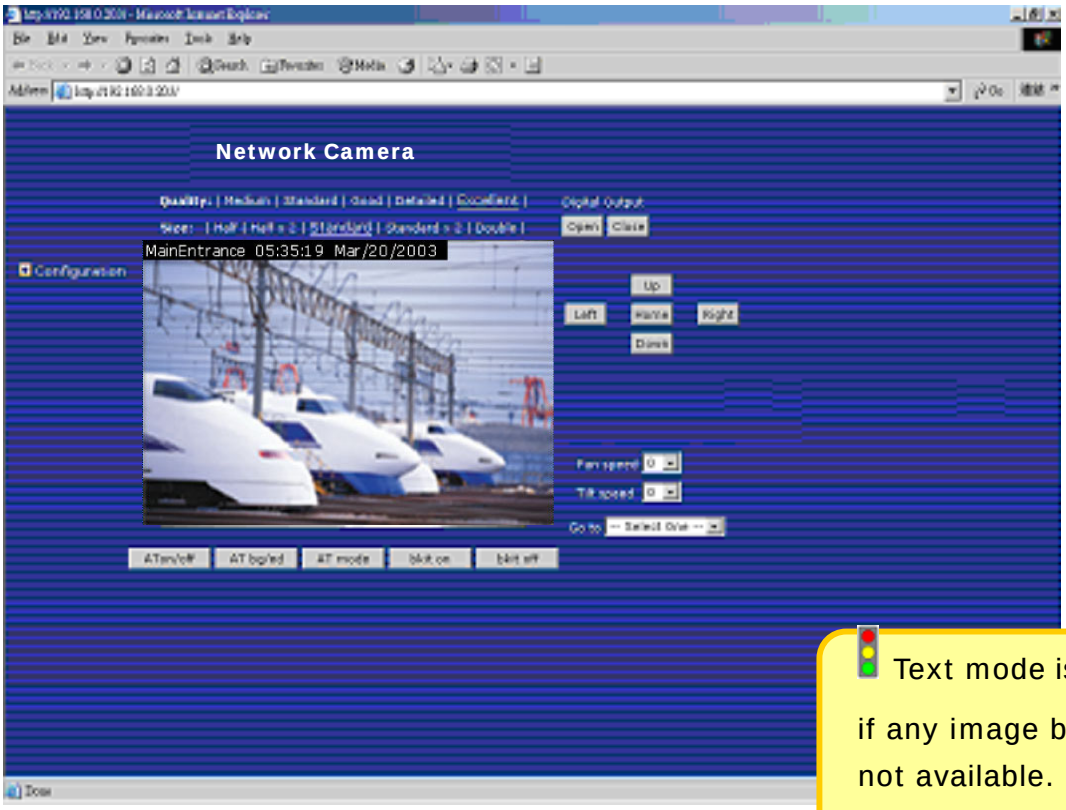
Main Page

Basic functions are displayed in main entrance page of Network Camera. The first figure below is graphic mode that has better visual effect and the second one is text mode that will shorten download time. The main page may look different depending on the PT scanner or the privilege of the user.

Graphic mode



Text mode



Video quality selection

It allows users to adjust the video quality for speed or smoothness. The performance is also subject to the network bandwidth and the number of users. Five options are available to be chosen from "**Medium**" to "**Excellent**". "**Medium**" quality means the picture has the quickest refresh rate but the worst image quality and "**Excellent**" quality means the picture has the slowest refresh rate but the best image quality.

Video size selection

It allows users to adjust the image size with consideration of bandwidth and image resolution. Five options are available including "**Half**", "**Half×2**", "**Standard**", "**Standard×2**" and "**Double**". "**Half×2**" consumes the same bandwidth as "**Half**" but has the same size with "**Standard**". Of course the visual effect is worse than "**Standard**". "**Standard×2**" compared to "**Double**" is similar to the case. "**Half×2**" is especially suits in the low bandwidth environment like a dial-up network. To fit into the small image area, timestamp will be skipped in "**Half**" and "**Half×2**" modes.

System configuration

There is a button or text link in the left side of the system configuration that only appears in administrators' main page.

External digital output control

There may be two remote control buttons for the each digital output on the main page. If there are external devices attached to the digital output, administrators or permitted users can click on Open to short "Common" and "Normal Open" pins of the digital output or click on Close to short "Common" and "Normal Close" pins of the digital output. To know more about the digital output for external devices, refer to the rear panel introduction of the Chapter Physical Description.

Motorized camera control

If there is any serial device like motorized camera attached and correctly setup to the COM port, the control panel will appear on permitted users' main page. The effective buttons will change color when users move the cursor over. Users can control the motorized camera in pan and tilt direction as well as zoom and focus. The home button can return the camera to the center position if the camera supports this command. Besides the near and far control in focus, an "AUTO" button is provided for setting auto focus mode. To move the motorized camera more precisely, speed control of pan and tilt allows users to fine tune the aiming position. Users also can directly click on any point in the image to force the motorized camera to focus on it. Users can pull down the list of preset locations to choose any one to move the camera to the preset location that is pre-defined by administrators. The detailed configurations are described in the related section in the Chapter Definitions of Configuration.

Custom camera commands

There are at most five buttons of custom commands for users to control the attached motorized cameras in addition to the default pan, tilt, zoom and focus control. The custom commands mean that administrators can setup some special commands like activating or deactivating the wiper of dome according to the user's manual of the attached motorized device.

System Configuration

Introduction

The system configuration can be easily done remotely on Internet Explorer through the Web interface. There are two wizards in addition to classified categories of system configurations. They can give friendly instructions and facilitate the setup job. Alternately administrators may type directly the URL of system configuration, "*http://<IP address of Network Camera>/setup/config.html*", to directly enter the configuration page. If administrators also want to set certain options through the URL, read the relative section in the Chapter Advanced Usage for reference. Network Camera also supports FTP to modify the system configuration file, CONFIG.INI, for technical usage. The details are described in the Chapter Advanced Usage.

Since it is a networking video server, administrators should run "**Setup wizard**" or well configure "**Security**", "**Network**" and "**Video**" at least. To support external serial port devices, configure "**COM port**" and then "**Camera Setting**" in "**Video**". To utilize the built-in features of security and web attraction, run "**Application wizard**" or configure "**Application**" and "**Demo**". Besides these features, administrators can adjust the system date and time in "**System**", or have different homepage layout by configuring "**Homepage layout**". Network Camera also provides some system maintenance like "**View log file**", "**View parameters**" and "**Factory default**".

Setup Wizard

The setup wizard will guide administrator to enter necessary information including system name, current date and time, administrator's password, video configuration and captions, and network settings. Administrators can exit the procedures anytime to reserve the current configuration. Finally the setup wizard will ask for reboot to validate the changes and administrators can decide to reboot later.

Application Wizard

There are two main applications including surveillance system and web attraction by means of Network Camera. The former one will utilize the built-in motion detection and external sensors to integrate with the existing e-mail or FTP server or external alarms to constitute a security system. It also possesses the weekly schedule for timed monitoring. The later one will customize the main page to your personal style and setup accounts for your possible visitors. The application is perfectly constructed and performed on several clicks by your fingertip. Administrators can additionally configure the application parameters in the Application page of configuration for more advanced usage after using Application wizard.

Definitions of Configuration

System parameters

Change host name

The “**host name**” is used for the homepage title of main page and displays as the title over the video window on the main page. The maximum string length is 40 characters or 20 characters in double-byte-character-systems like Chinese or Japanese.

Adjust date and time

There are three ways to adjust system date and time. The easiest is to make Network Camera "**Sync with computer time**". The second “**Manual**” is to set the date and time manually by entering new values. Notice the format in the related field while typing. The third “**Automatic**” is to make Network Camera automatically synchronize with timeservers over the Internet every month. It may fail if the assigned **NTP server** cannot be reached or Network Camera is within a local network. Leaving the NTP server blank will let Network Camera connect to default timeservers. Domain name or IP address format is acceptable as long as DNS server is available. Do not forget setting the "**Time zone**" offset for local settings. Refer to the Appendix G for the time zone of your region. It only affects the hour in NTP method.

“**Automatically restore DO state after seconds”** allows you to restore DO state after events trigger DO.

Once the settings are changed, click on

to validate changes.

Security privilege

Change root password

To change the administrator's password, type the new password in both text boxes identically. What is typed will be displayed as asterisks for security purposes. The maximum password is 16 characters. After pressing Save, the web browser will ask administrators for the new password for access.

Add new users

To add a new user, type the new user's name and password, check respective privilege, and then press Add to insert the entry. There are a total of twenty user accounts. Each user can have independent access right of the video channel, external I/O access and camera control.

Edit user's privilege

If the permitted rights of some user has to be changed, pull down the user list to find the user name and press Edit. A new window will pop out for administrators to change password and choose different privilege.

Delete existing users

To delete a user, pull down the user list to find the user name to be deleted and press Delete. A message window will pop up for confirmation.

Enable snapshot mode for more users

The maximum users that can view Network Camera at the same time are twenty. Administrators can check "**Allow more guests with snapshot mode**" to enable the snapshot mode for more users. Then the users over twenty will have the main page with snapshot mode instead of normal motion picture. It is practical for web attraction. In such case, configure the "**Snapshot interval**" to achieve better performance. The bigger interval between snapshots, the more users can have snapshot mode work.

Demonstration account

To setup Network Camera for demonstration to the public, administrators need to choose the service(s) to be permitted. After checking "view" in Security page , users may use "demo" as general user name and password is not required. Administrator also can assign the "Control Camera " or " Control Do" option to demo accout.To separate the demo account from primary users can prevent from interfering with the normal operations.

Network settings

Fix the IP address

To eliminate incautious mistakes during installation, Network Camera will stay in installation mode whenever it starts unless "**Reset network at next boot**" is disabled. This option can also be disabled using the Installer program. Once the option is disabled, Network Camera will skip installation at the next boot and the Installer program will not find the installed units. That implies that Network Camera cannot be accessed if no one remembers the IP address, except for restoring factory default settings. However, with this option disabled Network Camera can automatically operate normally after restarting in case of losing power. This option is ignored in the PPP connection.

Basic network settings

Administrators may need to modify the network settings to fit into existing networks. The subnet mask in some broadband service may differ from the default value 255.255.255.0 and service providers may assign more specific network settings. Administrators should change the configuration to what given by the service provider. The configuration may include "**IP address**", "**Subnet mask**", "**Default router**", "**Primary DNS server**" and "**Secondary DNS server**". After changing network settings, be sure to leave "**Reset network at next boot**" blank to skip next installation when the system restarts. Otherwise those network settings will be erased at the next start.

Changing port number of servers

For security or network integration, administrators also can hide the server from the general HTTP port by changing "**HTTP port**" to other than default 80. "**Local FTP server port"** can also be changed to other than default 21. Administrators should have enough network knowledge to change the default port.

E-mail settings

Network Camera not only plays the role of server, it will also actively connect to servers outside to send out messages or snapshots. When Network Camera starts, it will send out a system log via e-mail as long as the settings are correct rather than upload it via FTP. Even in modem application, Network Camera will send out a connection log whenever it dials out to an ISP or dialup server outside. If the administrator has setup some applications in either event mode or sequential mode, Network Camera will send out snapshots once conditions are met. To activate e-mail function, enter correct settings of "**SMTP (mail) server**" and "**Recipient email address**". "**Secondary SMTP (mail) server**" and "**Secondary email address**" are provided for backup connection when the primary one fails. "**Return email address**" is whom the mail will return when

the SMTP server rejects upon any failure. Some ISP may reject the mail if the address is invalid.

FTP settings

To send the log files described in the above paragraph via FTP, the SMTP server should be erased. Administrators must enter correct "**Primary FTP Server**", "**Primary FTP user name**" and "**Primary FTP password**". "**Primary FTP remote folder**" is the relative sub-folder in the remote FTP server. If the port of the remote FTP server is changed other than 21, set the real port to "**Primary FTP server port".** If the local network is protected by a firewall to prevent from initiating FTP connection from the remote FTP server, you may be able to connect to the FTP server but unable to put any file due to data channel connection failure. Check "**Primary FTP passive mode**" for passive transfer solution. Another set of "**Secondary**" server settings is also provided for backup connection.

In either e-mail or FTP, the primary server information should be entered first. If the primary server is not set, the related FTP or email will be cancelled. Note that it may take time to connect to the secondary server after the first one fails and it may affect some applications when conditions happen too often.

After everything is set, click on Save. A warning message will pop out for confirmation. After clicking on OK, Network Camera will automatically restart. If "**Reset network at next boot**" is kept checked, perform software installation again. Otherwise Network Camera will boot up according to the new configuration automatically.

Any change made to this page will make the system restart to validate. Make sure every field is correctly typed before clicking on Save. If Network Camera fails to response due to erratic settings, perform the restore procedures and run software installation.

Administrators should notice that the basic network settings including IP address, subnet mask, default router and DNS servers will be cleared when the network interface is switched to the other between Ethernet and modem.

Video and motion detection

Adjust image settings

"**Time stamp**" and "**Text on image**" will be enclosed in image for reference. The timestamp is captured from date and time of Network Camera that is maintained by an on-board real-time clock. "**Color**" setting is independent of the connected camera and "**B/W**" option can speed up the encoder a little. "**Default size**" option here will be the default size of video window when users first connect to Network Camera. "**Default quality**" option here will be the default quality when users first connect to Network Camera. And the "**Modulation**" type is auto-detected during initialization, but administrators can still set it manually. To adjust image settings for best visual quality, press Image Setting and a motion picture window will pop up for your reference. There are four fields including "**Brightness**", "**Contrast**", "**Hue**" and "**Saturation**" for video compensation. Each field has eleven levels ranged from -5 to +5. While adjusting, administrators can click on preview to check prior to Save the setting in memory. If the adjustment is not good, administrators can click on restore to restore the original settings without change. After configuration done, click on Close to close this window. If parameters are changed without saving, they will be used until the next system startup.

Maximum frame rate

This limits the maximal refresh frame rate.

Bandwidth utilization limit

Each Video Server can be limited in bandwidth utilization by administrators according to its priority and importance of location. "**Bandwidth limit**" is most useful to balance network utilization when multiple Video Server's are installed in the same network. It is more effective than changing image quality only and achieves better performance with adequate image size and quality.

Configure motion detection

The channel can have its own settings of motion detection independently. The settings including "**Object size**" and "**Sensitivity**" allow administrators fine tune to fit into the environment. The "**Object size**" decides the space ratio of motioned objects over the monitored screen. The "**Sensitivity**" sets the measurable difference between two sequential images that would indicate motion. The larger object size and lower sensitivity will make Network Camera ignore small variations in images. While the

motion amplitude of some object in the monitored screen is over the settings, a white M in red background will indicate at the upper-right corner of the window.
Motion detection is provided as reference because it is very environment-dependent. Especially working by the very sensitive settings, some triggered events may be considered as false alarms though there is tiny difference happening indeed. It can be affected by florescent light flashing, shadow shifting, and so on.

COM port configuration

Choose serial interface

There are two types of serial interfaces supported by COM port but only one interface can be used at one time. Administrators must set the correct "**Interface mode**" between RS232 and RS485 according to the attached device.

Choose device driver

If the attached device is PT scanner, administrators should select the appropriate model. Refer to our Web site for newly supported PT scanner. If the attached PT scanner is not in the support list, administrators can select "**Custom Camera**" to enter the proprietary commands for pan, tilt, zoom and focus control. If it is not a PT scanner but another serial device like video multiplexer, administrators can select the "**Generic CGI command**" to control the device via CGI commands. See the URL of External Device Control section in the Chapter Advanced Function for details.

COM port configuration

After saving the driver type, the COM port configuration will show up for entering the correct settings that depends on the camera type. Refer to the Appendix Settings for Supported PT scanner for default settings of supported PT scanner including baud rate, data bits, stop bit and parity bit.

Custom commands

Network Camera provides five more custom commands other than general pan, tilt, zoom and preset functions. Administrators can click on

and refer to the instruction manual of the attached device to setup frequently used functions. The "**Command**" should be entered in ASCII format; Network Camera will translate it into binary code and send it out through the serial port. For instance, a text string of "8101ABCDEF" will be translated into five bytes of hexadecimal 81, 01, AB, CD and EF. The maximal length of a command string is 60 which is equivalent to 30 hexadecimal bytes. "**Display string**" is for text on command buttons and should be less than 8 characters. If the "**Custom Camera**" is selected, there will be more commands for PTZF regarding to the custom camera.

ISP information setup

In PPP interface, a modem option will show instead of camera control 2. Configurations include modem initialization and outside dial-up server. If the users will setup with external sensors and alarms for property security, dial-out is needed to send some snapshot-attached e-mails when the preset conditions are triggered. In such applications, also remember to choose Network option to enter mail server address and recipient's e-mail address. If "**Dialout allowed**" is not checked, Network Camera will not send out any snapshots when events occur and the settings except for "**Initial modem command**" in this page will have no effect. The system will preset the attached modem to eliminate echo and mute line sound. To initialize the modem with further commands, type into the edit box. The prefix "AT" should be included.

Administrators should choose an appropriate "**Dial Method**" according to the local POTS environment. An incorrect dialing prefix may cause Network Camera to fail when dialing out. "**Redial attempts**" means how many times Network Camera should try to connect to each ISP. Setting the value in "**Disconnect after minutes**" will force Network Camera to drop the connection when there is no activity on the connection for the specific period. The range of this period is from 1 to 240 minutes, with 0 indicating a continuous connection. Administrators may let Network Camera keep the connection for a while to allow connections from outside. The IP address given by the ISP can be taken from the connection log that is mailed or uploaded when dial-up connection is successful. Setting the value to zero will make Network Camera always keep the connection.

Based on the settings of DI/DO in the application, the system will send mails or upload via FTP with image attachment upon the event occurring. In that case Network Camera will need a network connection and automatically dial out to the pre-configured server outside. When a connection is successfully established, Network Camera will send out a connection log to notify given network settings. For those installations that may switch the network interface between Ethernet and PPP, administrators should notice that the settings of FTP or SMTP servers might be different from what are in an Ethernet environment. If the network interface is changed, administrators may need to configure them in advance.

Network Camera will try the second ISP as a backup when the first ISP fails and exceeds the redial attempts. "**ISP phone number**" should be the complete phone number including country code and area code if necessary. "**Login username**" and "**Login password**" are used to pass the PPP negotiation requested by the ISP server. Note that

the pair of login name and password is dependent on the ISP and is different from what is used in the authentication process in web access.

Application constitution

Administrators can use combinations of options on the application page to perform many useful security applications. Network Camera provides two application modes; one is performed according to the settings on the web page, the other is performed according to the external command script. Though most settings will automatically be done by the Application Wizard, administrators still can adjust the settings from this page.

Weekly schedule

A useful weekly schedule is provided for daily security application. Administrators can select weekdays from Monday to Friday with the daily schedule from 9:00 am to 6:00 pm that no one is at home to perform any event checking. If the security system needs to be installed in office that no one is there during the nights or weekend, administrators just set the time period as above, then check "**All the time except for the above schedule**" for opposite operations.

External command script

Administrators can write a script named **SCRIPT.TXT** to perfectly match the additional software according to the Command Script for Complex Applications section in the Chapter Advanced Functions. After uploading this script to Network Camera via FTP, check the option "**Enable the external script file to exclude the following settings**". Otherwise Network Camera will operate according to the settings below.

Event operation

Network Camera provides general options for two basic applications, **event operation** for security and **sequential operation** for web attraction. In event operation, administrators have to setup some conditions to check and some actions to happen consequently. The conditions include motion detection and the status of digital input. While checking "Detect motion" box, administrators should click "Motion Detection" button on **Video** page or click "Motion Detection" link in **Applicatoin** page to configure the appropriate parameters. In the newly opened window, percentage of **object size** over whole window and **sensitivity** can be fine tuned to fit into the environment. If any motion is over the settings, an 'M' will appear on the upper-right corner of image for indication. The 'M' will appear in the image to indicate some motion is detected as long as "**Show alert in image**" is checked. If there are any sensors attached to the digital input, administrators can set the state to fire alarm. There are four states of "Input is **High**", "Input is **Low**", "Input is **Rising**" and "Input is **Falling**". The edge trigger like "Rising" or "Falling" is generally used to detect the emerging signal from the external sensor. Once any event happens, administrators can select "**Delay second(s) after**

event" option to drive some device attached to the digital output several seconds after the event happens and/or send snapshots that are taken right at the moment. . If administrators want to receive some snapshots to check the event, please check the "**Upload snapshot while input condition match**" box to get snapshots when inputting condition is matched the setting or check the "Upload snapshots while motion detected" box to get snapshot when motion has been detected. Network Camera will take three snapshots of pre-event, the moment of event, and post-event for video channel. Three snapshots of the channel can also be downloaded via FTP or HTTP URL. Refer to the Download Event-triggered Snapshots section for details.

Sequential operation

With this feature, Network Camera can upload snapshots periodically to external server as a live video source. The interval can be set from tenth second to several hours. The external server must be setup correctly in the Network configuration page.

Sending method

Either event mode or sequential mode can select one method between **email** and **FTP**. The companied external server must be setup correctly in advance. If email is chosen, the snapshots of the video channel will be attached in the emails. If FTP is chosen, administrators can choose to add date and time in the file name of snapshots. If the snapshots are used as the live video source, the date and time suffix can be eliminated to update the same source file.

The option "Show alert in image" may be set when running application wizard or configuring motion detection. Administrators should manually uncheck it if no indication of motion detection is needed in the image.

Homepage layout

There are two homepage display modes. One is "**Image mode**" that uses graphics for links; the other is "**Text mode**" that mostly uses text for links.

Administrators may easily give Network Camera a different presence of homepage. The "**logo graph**" for the system logo at the upper-left corner can be hidden; or the default image from the system memory can be used; or an external resource can be used by assigning a URL. The "**Background graph**" is similar. Default images of the system can be customized but limited by memory size. Images from external resources can be larger and more beautiful but will need more time to load. If the background is skipped, the background color will fill the browser window. Administrators also can give the system logo a "**Logo link**" to connect to another web site while clicked. The "**Font color**" and "**Background color**" can be chosen from sixteen colors as you like. See the Customize graphics in homepage section in the Chapter Advanced Functions for how to replace the default images of log, background and buttons of video switch.

If any necessary image is lost while homepage layout is image mode, Network Camera will switch to text mode automatically.

View log file

There is some useful information in the system log including current system configuration and activity history with timestamp for tracking.

View parameters

The whole system parameters will be categorized listed for administrators to check. The content is the same as CONFIG.INI.

Factory default

It is used to restore the factory default settings. This means any changes made before will be lost and the system will be reset to the initial status as shipping out of the factory. After confirmation, the system will restart and require the software installation to setup the network.

Advanced Functions

Capture Up-to-date Still Images

Get snapshot via URL

Administrator and users can use the specific URL to capture the current still image.

URL
http://<IP of Network Camera>/cgi-bin/video1.jpg[?<param>=<value>]

Get snapshot via FTP

Administrator and users can log-in the FTP daemon of Network Camera to download the refreshed JPEG image named **video.jpg**. The user name and password are as same as what in web access. The zero file size in file directory means it is captured by request.

Additional parameters:param	value	Description
quality	1	Medium
	2	Standard
	3	Good
	4	Detailed
	5	Excellent
size	1	Half
	2	Standard
	3	Double
	4	Halfx2
	5	Standardx2

Video Embedded in Customers' Homepage

In additional to the URL, some scripts should be added to download a plug-in for motion pictures. The following example simply displays title text and a real-time video window in Internet Explorer or Netscape. The user name and password should be configured in advance. Those who are familiar with HTML can easily add more components or rewrite a more vivid and useful homepage.

```
<html>
<head><title>Network Camera Sample Page</title></head>
<body>
<h2>Network Camera Sample Page</h2>
<script language="JavaScript">
<!--
if ((navigator.appName == "Microsoft Internet Explorer")&&(navigator.platform !=
"MacPPC"))  {
    document.write("<OBJECT ID=\"MjpegControl\" WIDTH=352 HEIGHT=240");
    document.write(" CLASSID=\"CLSID:EAA105FE-7BBD-4196-8B96-D46743894195
\" ");
    document.write("CODEBASE=\"http://username:password@192.168.0.201/plugin
/mjpegcontrol.cab#version=1,0,0,4\">");
    document.write("<PARAM NAME=\"VSize\" VALUE=\"2\">");
    document.write("<PARAM NAME=\"Url\" VALUE=\"http://username:password@
192.168.0.201/cgi-bin/video.jpg");
    document.write("?cam=1&quality=3&size=2\">");
    document.write("</OBJECT>");
  }  else  {
    document.write("<img width=352 height=240");
    document.write("src=\"http://192.168.0.201/cgi-bin/video.jpg?cam=1&quality=3
&size=2\">");
  }
//-->
</script>
</body>
</html>
```

Download Event-triggered Snapshots

There are three video image files for the video channel of three stages: pre-alarm, the moment when triggered and post-alarm. Only the snapshots captured by the last event are preserved. Administrator and users can use FTP or URL to get the saved snapshots. They can also be browsed from the application page in system configuration.

Get triggered snapshots via URL

/cgi-bin/snapshot.jpg?file=<value>

Video channel / Snapshot stage	Video
snapshot before event 5	Pre5
snapshot before event 4	Pre4
snapshot before event 3	Pre3
snapshot before event 2	Pre2
snapshot before event	Pre1
snapshot upon event	Trg1
snapshot after event	Pos1
snapshot after event 2	Pos2
snapshot after event 3	Pos3
snapshot after event 4	Pos4
snapshot after event 5	Pos5

Get triggered snapshots via FTP

File name	Pre-alarm	Upon alarm	Post-alarm
Video	vpre.jpg	vtrg.jpg	vpos.jpg
Video	vpre2.jpg		vpos2.jpg
Video	vpre3.jpg		vpos3.jpg
Video	vpre4.jpg		vpos4.jpg
Video	vpre5.jpg		vpos5.jpg

Uploading Snapshots Periodically

Upload snapshots to external FTP server

In sequential mode, Network Camera will send out snapshots according to interval and period settings. If snapshot files are intended for quick updates, it is better to skip date and time suffix. The file name will then be video1.jpg. If the snapshots are used for occasional monitoring, suffix with date and time can help administrators classify them easily.

Send snapshots to external SMTP (email) server

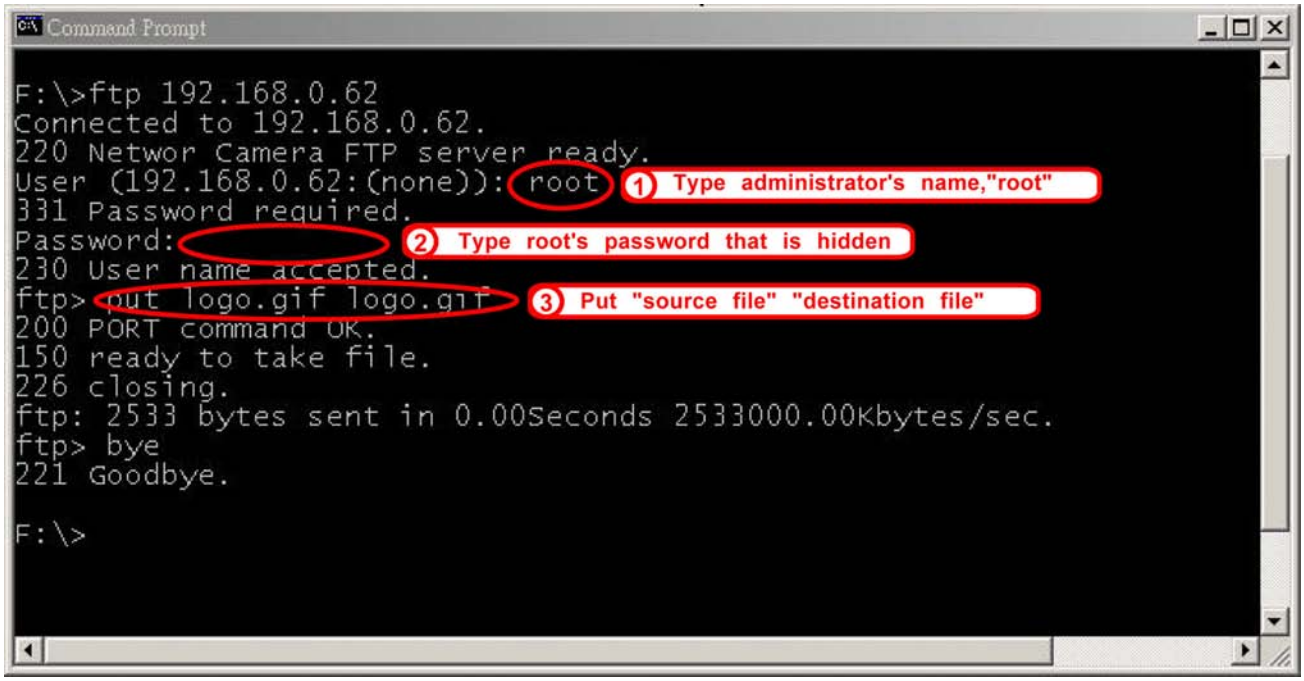
Comparing to the FTP method, email will induce more delay. But the email can notify users for prompt action.

Customize Graphics in Homepage

While in text mode, there is a small icon named BTN_TEXT.GIF preceding with each link that can be changed by administrators. While in image mode, the default method will use the image stored in Flash memory. The followings are the referenced file name and size limitation of each stored images. Administrators may customize preferred image under the size limit and put to the specific name via FTP. Administrators can download the original images before upload for backup.

Object	File name	Maximal size
Logo	logo.gif	Logo and background share 8000 bytes
Background	back.gif	Logo and background share 8000 bytes
Link icon	btn_text.gif	2000 bytes
Configuration	btn_conf.gif	5000 bytes

Usage via FTP is illustrated as below.



Command Script for Complex Applications

Besides the application wizard, Network Camera provides a more professional command script for advanced applications. The command script will be executed exclusively with the settings in Application page of system configuration except for the weekly schedule. To build the advanced application, follow the steps below.

1. Use any text editor to edit the appropriate command script according to the command format. The script size cannot exceed 500 bytes.
2. Save the script as a file named “SCRIPT.TXT”.
3. Use FTP with administrator’s privilege to upload the script file.
4. Enter the Application page in system configuration to define the time period in weekly schedule. If it is supposed to run any time, keep the original settings but check the option “All the time except for the above schedule”.
5. Check the option “Enable the external script file to exclude the following settings” to activate the command script.

Command format

[Event][“Operator”Event]……=[Action][+Action]……;

Event

[“Digital Input Number””Digital Input State”]
[“M” “Channel Number…”]
[“Channel Number””Video Input State”]

Operator

“+”: (OR)
“*”: (AND)

Action

[(“Delay Time”)“Digital Output Number””Digital Output State”]
[“V”“Channel Number”“P”“Preset Location Number”]
[“W”{“IP”:“Port”}{“Message”}]
[“U”“Method”]
[“S”“Channel Number…”]
[“N”{“filename”}];

Parameter explanation

Item between brackets means optional but at least one item should exist.

“Digital input number”: always 1

“Digital input state”:	H (high), L (low), / (low to high), \ (high to low)
“M”:	motion detection event.
“Channel Number”:	always A
“Video input state”:	/ (signal from loss to presence), \ (signal from presence to loss), X (as long as signal loss)
“Delay time”:	seconds of delay for the following actions after events happen
“Digital output number”:	always 1
“Digital output state”:	C (NC), O (NO)
“V”:	set video channel to go to preset location
“P”:	set preset location number to go to preset location
“W”:	send warning to server
“IP”:	server IP
“Port”:	server port
“Message”:	texts to be sent to the server
“U”:	upload snapshots
“Method”:	‘F’ is by FTP, ‘M’ is by e-mail
“S”:	take snapshot
“N”:	define the format of the filename
“;”:	end of line

The filename format is,

%a	image characterization (pre, trg, pos)
%y	year
%M	month
%d	day
%h	hour
%m	minute
%s	second
%t	tenth second

Practical examples

Command line	Description
M1=1C;	When any motion is detected, “Normal Close” of relay output will short with “Common”.
1\=(5)1O;	When DI transients from high to low, “Normal Open” of relay output will short with COMMON in 5 seconds.
A\=W{192.168.0.1:6000}{no signal!};	If there is no video signal, a message “no signal!” will be sent to port 6000 of 192.168.0.1 once.
1H=V1P15;	When sensor input 2 is high, drive the camera mapped to video 1 to go to preset location 16.
M1=UF+S1+N{video%c%a@%y%M%d%h%m%s};	If any motion is detected, upload snapshots. If an event triggered at 19:05:30 2002/10/15, the snapshot files will be named as, videopre@20021015190530.jpg, videotrg@20021015190530.jpg, videopos@20021015190531.jpg

The script file is limited to maximum 500 characters. The actual performance will depend on the complexity of the command script. Administrators should reduce the redundant check as possible. Overload conditional check and heavy actions may retard the system operation.

URL for External Device Control

Query status of digital input

/cgi-bin/getdi.cgi

Network Camera will return status of four digital input in one line.

Drive digital output

/cgi-bin/setdo.cgi?do1=<state>

<state>: ***C***, ***O*** denoting Normal Close or Normal Open respectively.

Move motorized camera in PT scanner direction

/cgi-bin/control.cgi?<param>=<value>&<param>=<value>……

param	**value**	**Description**
move	up	Tilt up
	down	Tilt down
	left	Pan left
	right	Pan right
	home	Return to home position
zoom	wide	Zoom in
	tele	Zoom out
focus	near	Focus near
	far	Focus far
	auto	Automatic focus
panspeed	-5 ~ 5	
tiltspeed	-5 ~ 5	

Recall camera position

/cgi-bin/recall.cgi?recall=<position>

<position>: the text string of a location that is preset in system configuration.

Refer to Camera preset configuration URL for preset function.

Transparent Remote Serial Driver

Network Camera provides a highly customized control support to third-party serial interface devices aside from PT scanner. That means in addition to setting up a custom camera with PTZF commands, users may utilize this mode and introduce a customized homepage to transmit arbitrary user-defined commands from user-side to Network Camera. The third-party device connected to the serial port of Network Camera will receive the same command sent by the originator. The user only needs to attach the command in ASCII format after the special URL. Network Camera will parse the commands and translate into binary code to send out.

Send command to device attached to COM port

/cgi-bin/senddata.cgi?data=123456,ABCDEF&flush=yes&wait=1000&read=6

This hyperlink will inform Network Camera to send out binary format commands to COM with “0x12, 0x34, 0x56” followed by “0xAB, 0xCD, 0xEF”. Each comma separates the commands by 200 milliseconds. “flush=yes” means the receive data buffer of COM port must be cleared before read. Then read 6 bytes after waiting for 1000 milliseconds. The read data can be up to 128 bytes and will return as ASCII coded hexadecimal value, e.g., 0x41, 0x42, 0x43 read from COM port will show in returned homepage as 414243 instead of ABC.

URL of System Maintenance

Download System Log via FTP

Besides viewing the system log from the web page, administrators can download the system log file, SYSTEM.LOG, via FTP. To log into the FTP daemon, enter “root” as the user name and the same administrator’s password used in Web access.

Restart System via URL

/cgi-bin/reset.cgi

Restart Network Camera without warning.

Restore Factory Default Settings via URL

/cgi-bin/restore.cgi

Network Camera will automatically restart after restoring factory default configurations.

Configure System via FTP

Administrators can use FTP to configure Network Camera much quicker than Web page especially for multiple targets. To configure system via FTP, first download the parameter file, CONFIG.INI, to customize each field according to the environment and then upload back to validate the new settings. To log into the FTP daemon, enter “root” as the user name and the same password used when connecting to the Web server. The serial number of Network Camera is the password for the initial access.

The file is composed of eight categories: [SYSTEM], [LAYOUT], [NETWORK], [VIDEO], [SERIAL1], [SERIAL2], [ALERT], and [DEMO]. The category name in brackets should be in upper case. The item name in angle braces should be in lower case. Some items related to disable/enable should use the keywords “YES”/“NO”. The number zero entry in <user name> and <user password> is for administrators, i.e. “root”. Basically Network Camera will restart automatically as soon as the file is accepted. If administrators want to cancel the reboot procedure, set the first item, <reset system> to NO. It will take effect once only and always show YES in the download file.

A sample CONFIG.INI is attached below. *The italic text* following each line describes the characteristic of the field and ***the bold italic characters*** are the options of the field.

```
Network Camera Initial Configuration File

    [SYSTEM]
    <reset system>                          or NO
    YES
    <host name>
    Network Camera                          string of maximum 40 characters
    <serial number>
    0002D1040011                            read-only
    <software version>
    IP21x1-VVTK-0202b                       read-only
    <current date>
    2004/06/08                              read-only
    <current time>
    12:34:56                                read-only
    <time zone>
    0                                       from 12 to -12
    <user name>
    (0)root                                 read-only
    (1)                                     string of maximum 16 characters
    (2)                                     the followings are as same as the above
    (3)
    (4)
    (5)
    (6)
```

(7)	
(8)	
(9)	
(10)	
(11)	
(12)	
(13)	
(14)	
(15)	
(16)	
(17)	
(18)	
(19)	
(20)	
<user password>	
(0)0002D1040011	*string of maximum 16 characters*
(1)	*the followings are as same as the above*
(2)	
(3)	
(4)	
(5)	
(6)	
(7)	
(8)	
(9)	
(10)	
(11)	
(12)	
(13)	
(14)	
(15)	
(16)	
(17)	
(18)	
(19)	
(20)	
<more guests enabled>	
NO	or ***YES*** *to enable snapshot mode*
<more guests interval>	
0	*seconds of snapshot interval*
[LAYOUT]	
<layout type>	
1	*image mode or* ***0*** *for text mode*
<font color>	***0****-black,* ***1****-white,* ***2****-green,* ***3****-maroon,* ***4****-*
1	*olive,* ***5****-navy,* ***6****-purple,* ***7****-gray,* ***8****-yellow,*
<background color>	***9****-lime,* ***10****-aqua,* ***11****-fuchsia,* ***12****-silver,*
0	***13****-red,* ***14****-blue,* ***15****-teal,*
<logo type>	
1	*default image, or* ***0*** *for blank, or* ***2*** *from URL*
<background type>	
1	*default image, or* ***0*** *for blank, or* ***2*** *from URL*
<logo source>	
http://	*URL of logo type 2, maximum 80 characters*
<background source>	
http://	*URL of logo type 2, maximum 80 characters*
<logo link>	
http://	*reference link of logo, max. 80 characters*

<com speedlink name>	
(0)	*string of maximum 8 characters*
(1)	*string of maximum 8 characters*
(2)	*string of maximum 8 characters*
(3)	*string of maximum 8 characters*
(4)	*string of maximum 8 characters*
[NETWORK]	
<install enabled>	
YES	*reset IP whenever system boots or **NO***
<ppp enabled>	
NO	*obsolete*
<ethernet address>	
00-02-D1-04-00-11	*read-only*
<host ip>	
192.168.0.207	*standard IP format*
<subnet mask>	
255.255.255.0	*standard IP format*
<gateway ip>	
0.0.0.0	*standard IP format*
<primary name server>	
0.0.0.0	*standard IP format*
<secondary name server>	
0.0.0.0	*standard IP format*
<ntp enabled>	
NO	*or **YES***
<network timing server>	*IP address or domain name*
<smtp mail server>	*IP address or domain name*
<mail recipient address>	*string of maximum 80 characters*
<smtp account name>	*string of maximum 63 characters*
<smtp password>	*string of maximum 16 characters*
<mail return address>	
Network Camera	*string of maximum 80 characters*
<backup smtp mail server>	*IP address or domain name*
<backup mail recipient address>	*string of maximum 80 characters*
<backup smtp account name>	*string of maximum 63 characters*
<backup smtp password>	*string of maximum 16 characters*
<local ftp port>	
21	*or **1024** ~ **65535***
<ftp server>	*IP address or domain name*
<ftp port>	
21	*or **1024** ~ **65535***
<ftp username>	*string of maximum 16 characters*
<ftp password>	*string of maximum 16 characters*

<ftp init path>	*string of maximum 40 characters*
<ftp passive> NO	*or **YES***
<backup ftp server>	*IP address or domain name*
<backup ftp port> 21	*or **1024 ~ 65535***
<bacup ftp username>	*string of maximum 16 characters*
<backup ftp password>	*string of maximum 16 characters*
<backup ftp init path>	*string of maximum 40 characters*
<backup ftp passive> NO	*or **YES***
<http server port> 80	*or **1024 ~ 65535***
<bandwidth limit> 0	*or **64000**, **128000**, **256000**, **512000**, **768000**, **1000000**, **1500000**, **2000000***
[VIDEO]	
<overlay timestamp> NO	*or **YES***
<caption text>	
<colored video> YES	*or **NO***
<video quality> 1	***1,2,3,4,5** representing Medium, Standard, GOOD, DETAILED, EXCELLENT*
<default size> 3	***1**-Half, **2**-Standard, **3**-Double, **4**-Halfx2 **5**-Standardx2*
<brightness> 0	*among **5** and **-5***
<contrast> 0	*among **5** and **-5***
<hue> 0	*among **5** and **-5***
<saturation> 0	*among **5** and **-5***
[SERIAL1]	
<data bits> 8	
<stop bits> 1	
<parity bits> 0	
<baud rate> 110	

```
<enable camera control>
10
<uart mode>
RS485                                   or RS232
<other control commands>
(0)                                     string of maximum 80 characters
(1)                                     string of maximum 80 characters
(2)                                     string of maximum 80 characters
(3)                                     string of maximum 80 characters
(4)                                     string of maximum 80 characters
<PT control commands>
HOME                                    string of maximum 80 characters

UP                                      string of maximum 80 characters

DOWN                                    string of maximum 80 characters

LEFT                                    string of maximum 80 characters

RIGHT                                   string of maximum 80 characters

[ALERT]
<script file enabled>
NO                                      or YES to activate external script
<motion detection channel enabled>
NO                                      or YES

<snapshot channel enabled>
NO                                      or YES
<series snapshot channel enabled>
NO                                      or YES
<application mode>
0                                       disabled, 1 for Sequential, 10 for motion
                                        detection event, 12 for DI event

<visual alert>
NO                                      or YES
<upload method>
0                                       FTP, 1 for email
<file with time suffix>
YES                                     or NO
<percentage of object size over screen>
10                                      1~99
<percentage of sensitivity>
90                                      1~99
<tenth seconds to snapshot after event>
5
<snapshots taken after event>
1
<time to start snapshot>
00:00:00                                24 hours format
<time to stop snapshot>
00:00:00                                24 hours format

[DEMO]
<demo enabled>
NO                                      or YES
<PTZ enabled>
```

NO *or* ***YES***<video is open>
NO *or* ***YES***

Telnet Commands

Network Camera has a Telnet daemon for only administrators to access some seldom used functions. Using any general terminal program to connect to Network Camera will prompt the user for a password. Username is not requested here since only administrators can access the Telnet daemon. The password is as same as that used in web access. After logging in, type "*help*" for the command list. If "*debug*" or "*dinote*" is not executed, Telnet will disconnect automatically after being idle for 1 minute.

System core debugging

General activities are recorded into SYSTEM.LOG continuously, but information about abnormal status is not. To look deep into the core debugging information, administrators may type the "*debug*" command. This will cause Network Camera to start dumping the detailed debugging information while the system is running. This is useful to examine if any error has occurred when the system operates abnormally. The stored information will be cleared automatically after the dump. Network Camera will continue to dump new messages unless the connection is broken. If Telnet is not connected, any messages will be stored until administrators re-login.

Monitor changed status of digital input

Typing "*dinote*" will make Network Camera send the current status of all digital input. After that Network Camera will continuously monitor DI status and send messages only when the state has changed. For example, after typing "*dinote*" the terminal will display
DI1=L
and after DI2 changes to H, terminal will display
DI1=H

Stop information dumping

Typing "*stop*" will cease dumping debug information and the digital input status.

Query status of digital input

Typing "*diquery*" will display the status of all digital input once.

Set digital output

To set digital output to connect NO with COMMON, type "DO1=L".
To set digital output to connect NC with COMMON, type "DO1=H".

Erase snapshots stored in Flash memory

Typing "*erase image*" will clear all snapshots saved in Flash memory.

Erase logo and graphic buttons

Typing "*erase graph*" will clear all images used on the homepage. If no new images are uploaded, the system will switch to text mode and use default images instead.

Skip installation at next boot

Typing "*lock*" will inform Network Camera to fix current network settings. It need not wait for installation during the next boot.

Reset network for new settings

Typing "*unlock*" will make Network Camera give up current settings and wait for installation.

Restore factory default settings

Typing "*clear*" will make Network Camera restore factory settings but not restart. To validate new settings, type "reset" to make the system restart.

Reset system

Typing "*reset*" will make Network Camera perform a software reset.

Appendix

A. Troubleshooting

Power-On-Self-Test

After the power has been turned on, Network Camera will perform a self-diagnostic to detect any possible hardware defects. If the power indicator is dim at the beginning, the system fails to proceed further without power. While the POST is proceeding, the status LED indicators will keep blinking interchanged until finished or any fatal error happens. If either status LED indicator is dim at the beginning, the LED may be broken.

Any possible fatal error has a special pattern shown in the following table. LED1 is the one below power indicator and LED2 is the lowest one.

LED pattern after POST	Failed function	Troubleshooting
LED2 and LED3 blink at same time	Video input	The video decoder is broken. Ask your reseller for technical service.
LED2 ON and LED3 OFF	Ethernet network	The PCI interface cannot work. Ask your reseller for technical service.
LED2 OFF and LED3 ON	Ethernet network	The Ethernet controller is broken. Ask your reseller for technical service.
LED2 ON and LED3 ON	Ethernet interface	Ethernet interface failure includes not only components on board but also Ethernet cable and the devices of the opposite end.
LED2 blink and LED3 ON	System date and time	The real-time clock is broken. Ask your reseller for technical service.
LED2 ON and LED3 blink	Camera control via COM or modem interface	The UART controller is broken. Ask your reseller for technical service.

To reduce the system failure caused by operation error, always read the related sections in this user's manual to prevent from unexpected error caused by wild-guess configuration.

B. Frequently Asked Questions

Q Why can't I see the Network Camera in the installer after reboot?
A The installer is only used to install the IP address of Network Camera. If the IP address is fixed by checking the option in the installer, the Network Camera will no longer appear in the installer.

Q Why can't I connect the Network Camera after reboot?
A If the IP address is not fixed, Network Camera will always wait for installing command for a valid IP address. That means the previous IP address will not be used if the option in the installer is not checked; or the option in the network configuration is not cleared. The benefit of waiting for a valid IP address by default is that administrators can find the Network Camera in the installer to prevent IP conflict. As long as the IP address is confirmed, it is suggested to fix the IP address to make Network Camera automatically start up whenever regaining power.

Q What if I forget my password?
A Every access to Network Camera needs authentication. If you are not a permitted user, you may view the images or control the camera as long as the demo account is opened. The demo account user may use username as "demo" without any password to access limited features. If you are one of the managed users, you have to ask the administrators for the password. If you are the administrator, there is no way to recover the root password. The only way to regain access to Network Camera is to restore the factory settings and reinstall it.

Q Why can I not watch video from Network Camera after it is authenticated?
A There are many possible scenarios regarding this problem,
1. If you have just installed Network Camera and are unable to watch the video, check if the video input is enabled and the video modulation in Configuration page.
2. If Network Camera is well installed and you are accessing Network Camera for the first time using Internet Explorer, adjust the security level of Internet Explorer to allow installation of the plug-in.
3. If the problem still exists after adjusting, the current users may be over the system allows.
4. In case that you use demo account, the administrator may protect the video from the public.

Q How can I use a name instead of the IP address to connect Network Camera?
A To allow users to connect to Network Camera through an easily memorized name, the administrators must first configure the name server in his network. Here is an example: the administrator installs the Network Camera with a reserved IP address and assigns it with a name in the domain name service, then users can connect to Network Camera by typing a name instead of IP address. If there is DHCP service in the network, the IP address must be excluded in the DHCP service to prevent from IP conflict.

Q What is the plug-in for?
A The plug-in provided by Network Camera is used to display motion pictures on Internet Explorer that does not support server push technology. If your system does not allow installation of any plug-in software, the security level of web browser may need to be lowered. It is recommended that you consult your network supervisor in your office regarding the adjustment of the security level.

Q Why is the timestamp different from the system time of my PC or notebook?
A The timestamp is based on the system time of Network Camera. It is maintained by a real-time clock inside and automatically synchronizes with the time server if Network Camera is connected to the Internet and the function is enabled. Differences of several hours may result from the time zone setting.

Q Why does the image not refresh regularly?
A In a modem environment, it is because the bandwidth of PPP connection is far less than Ethernet. If the difference of the timestamp is not stable, adjust the UART FIFO lower in both receiving and transmitting from modem property in the control panel. While in Ethernet, it may be due to time taken in storing snapshots into memory upon events occurring.

Q How many users are allowed to watch Network Camera at the same time?
A To achieve the best effect, Network Camera will allow twenty users to connect at the same time. Excess users can get an auto-refreshed still image in homepage instead. It is recommended to build another web server to host a large quantity of users by retrieving images from Network Camera periodically.

Q How fast is the video rate of Network Camera?
A The JPEG codec can process 30 frames per second internally. However the total performance is subject to many coefficients as follows,
1. network throughput,

2. bandwidth share,
3. number of users,
4. number of video input is accessed at one time,
5. the complicated objects in view results in larger image file,
6. the level of your PC or notebook which is responsible of displaying images.
In general, the transfer rate in general local network environment can achieve over 200 kilobytes per second and approximately 10 to 20 pictures of normal environment per second. The general frame size is illustrated in the follow table for reference.

Quality setting	Size of each frame	Bandwidth demand for 30fps
Medium	9.3 kbyte	2246 kbps
Standard	11.15 kbyte	2676 kbps
Good	13.76 kbyte	3303 kbps
Detailed	16.35 kbyte	3925 kbps
Excellent	20.3 kbyte	4886 kbps

Q How can I keep Network Camera as private as possible?
A Network Camera is designed for surveillance purpose and has many flexible interfaces. The user authentication and special confirmation in installation can keep Network Camera from unauthorized access. You may also change the HTTP port to non-public number. You can check system log to examine any abnormal activities and trace the origins.

Q Why can I see image files when I use dir in FTP even if the alarm is not triggered?
A Every time Network Camera starts, it will capture the images as vpre.jpg. If there are previously saved image files that are not retrieved, Network Camera will keep them until they are accessed.

Q How will the stored images be processed if Network Camera loses power?
A If user has defined the snapshot interval, Network Camera will capture images periodically. Once the pre-defined condition is match, the pre-alarm images will be kept and the current images will be saved. The subsequent images will be stored as post-alarm stage. User may retrieve these files either by downloading via FTP or direct Network Camera send them in e-mails. That means after monitoring conditions are met, Network Camera will keep these image files until user retrieval even if power is lost.

Q If I set Network Camera to send e-mails of images whenever the conditions are met, will my e-mail account overflow?
A It is recommended to use transient state rather than steady state. For instance, use

‘Input is Rising’ and ‘Input is Falling’ rather than ‘Input is High’ and ‘Input is Low’ to let the condition be triggered only when state is changed.

Q The image is not clear enough. Is anything broken?
A The lens can be fine adjusted by rotating the outer ring. Please rotate it clockwise or counter-clockwise to focus near or far.

C. Upgrade System Firmware

Customers can frequently check the appropriate product folder on our web site to download the latest firmware. Only administrators can upgrade the system firmware of Network Camera.

Easy way via Upgrade Wizard

Run the Upgrade Wizard included in the product CDROM and proceed by the prompts. Refer to the user's guide of Upgrade Wizard for details.

Alternative via FTP

1. Decompress the compressed file in a local folder. A file named FLASH.BIN should appear.
2. Use the FTP program and change the working directory to the local folder where FLASH.BIN exists.
3. Connect to Network Camera with user name as “root” and password.
4. Use the PUT command to upload FLASH.BIN to Network Camera. The file size is near 1.5 mega bytes. It will take approximately 2 seconds in a local network, 2 minutes by null modem connection or 6 minutes by modem, but still subject to user's network.
5. After upload is complete, close the connection.
6. If the received FLASH.BIN is checked without error, Network Camera will update the software in Flash memory and restart automatically. When Network Camera starts writing firmware, both status LED indicators will stay on until system restarts. It takes about 30 to 40 seconds. User must keep the power stable during the update process. After the system restarts, Network Camera may need installation depending on whether the “Reset network at next boot” option is enabled or not. After Network Camera boots up, reload the web page in the browser.

If power fails during the software upgrade, the program in the memory of Network Camera may be destroyed permanently. If Network Camera cannot restart properly, ask the dealer for technical service.

D. URL Commands of Network Camera

For some customers who already have their own web site or web control application, Network Camera can be easily integrated through convenient URL. This section lists the commands in URL format corresponding to the basic functions of Network Camera. Some RFC standards related to HTML may be a good reference for implementation of the customized homepage.

Page URL

The configuration page has a frame layout including option list frame and an option page frame. Referenced URL except for the configuration page directs to option page frame only. Some pages, like image quality setting and preset setting, are opened in new windows for preview.

These URLs can be accessed only by administrators.

Homepage name	Referenced URL
configuration page	/setup/config.html
system option	/setup/system.html
security option	/setup/security.html
network option	/setup/network.html
video option	/setup/video.html
image quality option	/setup/image.html
camera control	/setup/serial.html
preset PT scanner	/setup/preset.html
custom command setting	/setup/cuscom.html
custom camera setting	/setup/custom.html
application option	/setup/app.html
motion detection setting	/setup/motion.html
view snapshots	/setup/snap.html
demo option	/setup/demo.html
homepage layout option	/setup/layout.html
system log	/setup/logfile.html
system parameters	/setup/parafile.html
set factory default	/setup/factory.html

System resource URL

There are some images used on the homepage when the homepage layout is in image mode. Administrators may use the following links to show the images saved in Network Camera on another page. To change the logo or the background images referenced by the URL, refer to the homepage layout section in configuration.

Resource name	Referenced URL
system logo image	/logo.gif
background image	/back.gif
button image for configuration	/btn_conf.gif
icon image for link indicator	/btn_text.gif

General format of command URL

Every configuration can be set through URL with POST method by administrators only.

<general format>

URL[?[name=value][&name=value]……]

<method>

POST

<authorized user>

root

System configuration URL

URL: /cgi-bin/system.cgi

NAME	VALUE	DESCRIPTION
host	<text string shorter than 15 characters>	system name
method	keep	keep date and time unchanged
	auto	use NTP server to synchronize
	manu	directly adjust date and time
date	<yy/mm/dd>	year, month and date separated by slash
time	<hh:mm:ss>	hour, minute and second separated by colon
ntp	<domain name or IP address>	NTP server
zone	GMT±<n>:00	time zone, n ranged from 0 to 12

Security configuration URL

URL: /cgi-bin/security.cgi

NAME	VALUE	DESCRIPTION
rootpass	<text string shorter than 15 characters>	change root password
username	<text string shorter than 15 characters>	add new user
userpass	<text string shorter than 15 characters>	new user's password
ioallowed	<not required>	allow user to control DO
ptzallowed	<not required>	allow user to view PT scanner panel
deluser	<text string shorter than 15	Existing user name

	characters>	
slow	<not required>	Snapshot mode
open	<not required>	enable demo account
camctrl	<not required>	allow demo user to control the PT scanner
demoioallowed	<not required>	allow demo user to control the I/O access
slow	<not required>	snapshot mode
delay	<integer>	refresh time in snapshot mode

Network configuration URL

URL: /cgi-bin/network.cgi

NAME	VALUE	DESCRIPTION
reset	yes	enable installation at next boot
	<other than yes>	disable installation at next boot
ip	<IP address>	Network Camera's IP address
subnet	<IP address>	subnet mask
router	<IP address>	default gateway
domain	<text string shorter than 40 characters>	domain name of Network Camera
dns1	<IP address>	primary DNS server
dns2	<IP address>	secondary DNS server
limit	Not limited	use full network bandwidth
	64Kbits/second	use only 64Kbps of bandwidth
	128Kbits/second	use only 128Kbps of bandwidth
	256Kbits/second	use only 256Kbps of bandwidth
	512Kbits/second	use only 512Kbps of bandwidth
	768Kbits/second	use only 768Kbps of bandwidth
	1Mbits/second	use only 1Mbps of bandwidth
	1.5Mbits/second	use only 1.5Mbps of bandwidth
	2Mbits/second	use only 2Mbps of bandwidth
http	<number less than 65535>	HTTP port
smtp1	<domain name or IP address>	primary SMTP server
mailto1	<text string shorter than 80 characters>	mail recipient address
smtp2	<domain name or IP address>	secondary SMTP server
mailto2	<text string shorter than 80	mail recipient address

	characters>	
returnmail	<text string shorter than 80 characters>	return address
ftp1	<domain name or IP address>	primary FTP server
ftprp1	<number less than 65535>	FTP server port
ftpuser1	<text string shorter than 15 characters>	user name for primary FTP server
ftppass1	<text string shorter than 15 characters>	password for primary FTP server
ftpfolder1	<text string shorter than 40 characters>	upload folder in primary FTP server
ftp2	<domain name or IP address>	secondary FTP server
ftprp2	<number less than 65535>	secondary FTP server port
ftpuser2	<text string shorter than 15 characters>	user name for secondary FTP server
ftppass2	<text string shorter than 15 characters>	password for secondary FTP server
ftpfolder2	<text string shorter than 40 characters>	upload folder in secondary FTP server

Video configuration URL

URL: /cgi-bin/video.cgi

NAME	VALUE	DESCRIPTION
time	<not required>	enclose timestamp
text	<text string shorter than 15 characters>	enclose caption
color	B/W	set encoder to monochrome
	<other than B/W>	set encoder to color
size	Half	set size to half
	Standard	set size to standard
	Double	set size to double
	Half x 2	set size to half x 2
	Standard x 2	set size to standard x 2
quality	Medium	lowest resolution
	Standard	lower resolution
	Good	normal setting
	Detailed	higher resolution
	Excellent	highest resolution

Image quality configuration URL

URL: /cgi-bin/image.cgi

NAME	VALUE	DESCRIPTION
brightness	<-5 ~ 5>	adjust brightness of image
contrast	<-5 ~ 5>	adjust contrast of image
hue	<-5 ~ 5>	adjust hue of image
saturation	<-5 ~ 5>	adjust saturation of image
preview	<not required>	not save the parameters
restore	<not required>	recall the original settings
save	<not required>	save the parameters

Motion detection configuration URL

URL: /cgi-bin/motion.cgi

NAME	VALUE	DESCRIPTION
per	<integer>	object size percentage
sen	<integer>	sensitivity percentage

COM configuration URL

URL: /cgi-bin/serial1.cgi

NAME	VALUE	DESCRIPTION
interface	RS232	switch COM to RS232
	RS485	switch COM to RS485
detect	generic	accept generic CGI commands
	modem	use modem
	none	no drivers
driver	Sony VISCA	
	Canon VCC1	
	Canon VCC3	
	Canon VCC4	
	DynaDome/SmartDOME	
	Pelco D protocol	
	Lilin PIH-7x00	
	Ernitec	
	Custom Camera	third party PT scanner

Custom camera configuration URL

URL: /cgi-bin/serialportsettings.cgi

NAME	VALUE	DESCRIPTION
baud1	<integer>	set baud rate of COM
data1	<integer>	set data bits of COM
stop1	1	set 1 stop bit of COM
	2 <other than 1>	set 2 stop bits of COM
parity1	None	set parity check of COM to none
	Odd	set parity check of COM to odd
	Even	set parity check of COM to even

Camera custom command configuration URL

URL: /cgi-bin/cuscom.cgi

NAME	VALUE	DESCRIPTION
up1	<text string shorter than 80 characters>	tilt up command string of COM
down1	<text string shorter than 80 characters>	tilt down command string of COM
left1	<text string shorter than 80 characters>	pan left command string of COM
right1	<text string shorter than 80 characters>	pan right command string of COM
home1	<text string shorter than 80 characters>	home command string of COM
tele1	<text string shorter than 80 characters>	zoom in command string of COM
wide1	<text string shorter than 80 characters>	zoom out command string of COM
str11	<text string shorter than 8 characters>	button name of custom command 1 of COM
str12	<text string shorter than 8 characters>	button name of custom command 2 of COM
str13	<text string shorter than 8 characters>	button name of custom command 3 of COM
str14	<text string shorter than 8 characters>	button name of custom command 4 of COM
str15	<text string shorter than 8 characters>	button name of custom command 5 of COM
com11	<text string shorter than 80 characters>	custom command 1 of COM
com12	<text string shorter than 80 characters>	custom command 2 of COM
com13	<text string shorter than 80 characters>	custom command 3 of COM
com14	<text string shorter than 80 characters>	custom command 4 of COM
com15	<text string shorter than 80 characters>	custom command 5 of COM

Modem configuration

URL:/cgi-bin/serialmodem.cgi

NAME	VALUE	DESCRIPTION
dialout	yes	allow Network Camera dialing out on event
	no	no dial-out allowed
method	Tone (ATDT)	make modem dial in tone
	Pulse (ATDP)	make modem dial in pulse
reatt	<integer>	redial attempts
discon	<integer>	minutes delay before disconnection
init	<text string shorter than 40 characters>	command to initialize modem
phone1	<text string shorter than 40 characters>	phone number of primary ISP
user1	<text string shorter than 40 characters>	user name for primary ISP
pass1	<text string shorter than 40 characters>	password for primary ISP
phone2	<text string shorter than 40 characters>	phone number of secondary ISP
user2	<text string shorter than 40 characters>	user name for secondary ISP
pass2	<text string shorter than 40 characters>	password for secondary ISP

Application configuration URL

URL: /cgi-bin/app.cgi

NAME	VALUE	DESCRIPTION
sun	<not required>	set Sunday in weekly schedule
mon	<not required>	set Monday in weekly schedule
tue	<not required>	set Tueday in weekly schedule
wed	<not required>	set Wednesday in weekly schedule
thu	<not required>	set Thursday in weekly schedule
fri	<not required>	set Friday in weekly schedule
sat	<not required>	set Saturday in weekly schedule
sbegin	<hh:mm:ss>	time to start in weekly schedule
send	<hh:mm:ss>	time to stop in weekly schedule
inv	<not required>	set inverse mode in weekly schedule

enfile	<not required>	enable script file
emode	<not required>	event operation
showalert	<not required>	show alert in image
mdmode	<not required>	Enable motion detection
dihigh	<not required>	Enable DI is high
dilow	<not required>	Enable DI is low
dirise	<not required>	Enable DI is rising
difall	<not required>	Enable DI is falling
delay	<integer>	delay time of DO after event
ioalarm	<not required>	trigger DO when DI condition matched
mdalarm	<not required>	trigger DO when motion detected
ioupload	<not required>	upload snapshot when DI condition matched
mdupload	<not required>	upload snapshot when motion detected
resetdo	<not required>	Clear the DO status
smode	<not required>	sequential mode application
sinter	<integer>	tenth seconds interval for sequential mode
smethod	mail	upload snapshots by email
	ftp	upload snapshots by FTP
suffix	<not required>	FTP file with date and time suffix

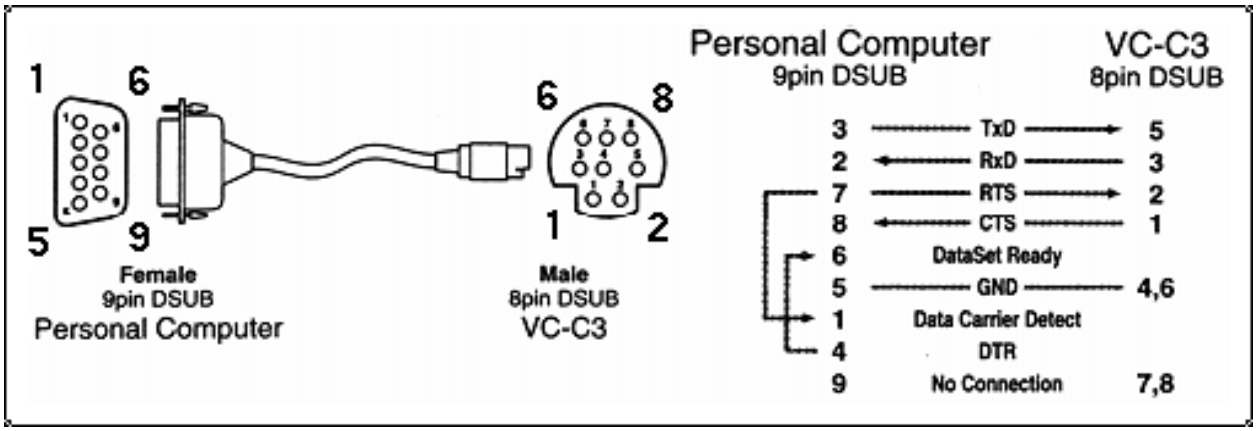
Homepage layout configuration URL

URL: /cgi-bin/layout.cgi

NAME	VALUE	DESCRIPTION
cuslogo	blank	hide logo
	def	use default logo
	url	use image from URL
logourl	<text string shorter than 80 characters>	URL of image for logo
linkurl	<text string shorter than 80 characters>	URL to link when clicking on logo
cusback	blank	hide background image
	def	use default background
	url	use image from URL
backurl	<text string shorter than 80 characters>	URL of image for background
fcolor	<0 ~ 15>	color index for font
bcolor	<0 ~ 15>	color index for background
dismode	image	display homepage in image mode
	text	display homepage in text mode

E. Camera Control Cable

The included cable can be used to control motorized cameras of desktop types from Sony and Canon. The pin assignment is illustrated in the following chart. To control cameras of another brand, check the user's manual of the motorized camera if the pin assignment of the control cable is appropriate.



F. Time Zone Table

While setting the time zone in automatic date/time synchronization, find the hour offset in the followings for your region. GMT stands for Greenwich Mean Time, which is the global time that all time zones are measured from.

(GMT–12:00)	International Date Line West
(GMT-11:00)	Midway Island, Samoa
(GMT-10:00)	Hawaii
(GMT-09:00)	Alaska
(GMT-08:00)	Pacific Time (US & Canada), Tijuana
(GMT-07:00)	Arizona
(GMT-07:00)	Chihuahua, La Paz, Mazatlan
(GMT-07:00)	Mountain Time (US & Canada)
(GMT-06:00)	Central America
(GMT-06:00)	Central Time (US & Canada)
(GMT-06:00)	Guadalajara, Mexico City, Monterrey
(GMT-06:00)	Saskatchewan
(GMT-05:00)	Bogota, Lima, Quito
(GMT-05:00)	Eastern Time (US & Canada)
(GMT-05:00)	Indiana (East)
(GMT-04:00)	Atlantic Time (Canada)
(GMT-04:00)	Caracas, La Paz
(GMT-04:00)	Santiago
(GMT-03:30)	Newfoundland
(GMT-03:00)	Brasilia
(GMT-03:00)	Buenos Aires, Georgetown
(GMT-03:00)	Greenland
(GMT-02:00)	Mid-Atlantic
(GMT-01:00)	Azores
(GMT-01:00)	Cape Verde Is.
(GMT)	Casablanca, Monrovia
(GMT)	Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London
(GMT+01:00)	Amsterdam, Berlin, Bern, Stockholm, Vienna
(GMT+01:00)	Belgrade, Bratislava, Budapest, Ljubljana, Prague
(GMT+01:00)	Brussels, Copenhagen, Madrid, Paris
(GMT+01:00)	Sarajevo, Skopje, Warsaw, Zagreb

(GMT+01:00) West Central Africa
(GMT+02:00) Athens, Istanbul, Minsk
(GMT+02:00) Bucharest
(GMT+02:00) Cairo
(GMT+02:00) Harare, Pretoria
(GMT+02:00) Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius
(GMT+02:00) Jerusalem
(GMT+03:00) Baghdad
(GMT+03:00) Kuwait, Riyadh
(GMT+03:00) Moscow, St. Petersburg, Volgograd
(GMT+03:00) Nairobi
(GMT+03:30) Tehran
(GMT+04:00) Abu Dhabi, Muscat
(GMT+04:00) Baku, Tbilisi, Yerevan
(GMT+04:30) Kabul
(GMT+05:00) Ekaterinburg
(GMT+05:00) Islamabad, Karachi, Tashkent
(GMT+05:30) Chennai, Kolkata, Mumbai, New Delhi
(GMT+05:45) Kathmandu
(GMT+06:00) Almaty, Novosibirsk
(GMT+06:00) Astana, Dhaka
(GMT+06:00) Sri Jayawardenepura
(GMT+06:30) Rangoon
(GMT+07:00) Bangkok, Hanoi, Jakarta
(GMT+07:00) Krasnoyarsk
(GMT+08:00) Beijing, Chongqing, Hongkong, Urumqi
(GMT+08:00) Taipei
(GMT+08:00) Irkutsk, Ulaan Bataar
(GMT+08:00) Kuala Lumpur, Singapore
(GMT+08:00) Perth
(GMT+09:00) Osaka, Sapporo, Tokyo
(GMT+09:00) Seoul
(GMT+09:00) Yakutsk
(GMT+09:30) Adelaide
(GMT+09:30) Darwin
(GMT+10:00) Brisbane
(GMT+10:00) Canberra, Melbourne, Sydney
(GMT+10:00) Guam, Port Moresby

(GMT+10:00) Hobart
(GMT+10:00) Vladivostok
(GMT+11:00) Magadan, Solomon Is., New Caledonia
(GMT+12:00) Auckland, Wellington
(GMT+12:00) Fiji, Kamchatka, Marshall Is..
(GMT+13:00) Nuku'alofa

G. Technical Specifications

System
CPU: Trimedia PNX1300
RAM: 16MB SDRAM
ROM: 2MB FLASH ROM

Networking
Adjustable bandwidth limit

Protocol
TCP/IP, HTTP, SMTP, FTP, Telnet, NTP, DNS and DHCP

Modem
PPP (dial-up, direct cable connection)

Physical
10BaseT Ethernet or 100BaseT Fast Ethernet

Video

Algorithm Supported
MJPEG

Features
Adjustable image size and quality
B/W or color control
Timestamp and text overlay

Resolution
IP2111
Up to 30 frames at 176x112
Up to 30 frames at 352X240
Up to 9 frames at 704X480
IP2121
Up to 25 frames at 176x144
Up to 25 frames at 352X288
Up to 8 frames at 704X576

Camera Specification
1/3 inch cooler CCD image sensor
1 Lux/F2.0
AGC, AWB, AES
IP2111
- Resolution: 512(H)x492(V)
- Electroic shutter. 1/60 ~ 1/100.000sec

IP2121
- Resolution: 512(H)x492(V)
- Electroic shutter. 1/50 ~ 1/100.000sec

Serial Port
9 pin D-SUB RS232 or RS485 (PTZ camera control) max.115.2Kbps

General I/O
1 sensor inputs (max. 12VDC 50mA)
1 relay outputs (max. 24VDC 1A, 125VAC 0.5A)

LED Indicator
System power and status indicators
Network link and speed indicators

Dimension
143.6mm (L) * 93.8mm (W) * 71.6mm (H)

Weight
Net. 700g.

Power
Consumption: near 5.4W
Input: 100-240VAC, 50/60Hz, 0.4A
Output: 12VDC, 1.5A

Operating Environment
Temperature: 0-50°C/32-122°F
Humidity: 95%RH

EMI & Safety
CE, FCC

Viewing System Requirement
Internet Explorer 4.x or above,
Netscape Navigator 4.x or above

Electromagnetic Compatibility (EMC)

USA - This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a partial installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

-- Reorient or relocate the receiving antenna.

-- Increase the seperation between the equipment and receiver.

-- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

-- Consult the dealer or an experienced radio/TV technician for help.

Shielded interface cables must be used in order to comply with emission limits.

Europe CE - This digital equipment fulfills the requirement for radiated emission according to limit B of EN55022/1998, and the requirement for immunity according to EN50082-1/1992.

Liability

Vivotek Inc. cannot be held responsible for any technical or typographical errors and reserves the right to make changes to the product and manuals without prior notice. Vivotek Inc. makes no warranty of any kind with regard to the material contained within this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose.